Patrick Gray
Principal Security Strategist
Cisco

HACKERS, CRACKERS, BOTS, MALWARE AND PHISHERS, OH MY!

It’s a great to be in Sacramento today, but uh, do you know where your data is right now?

It’s all about data, your data

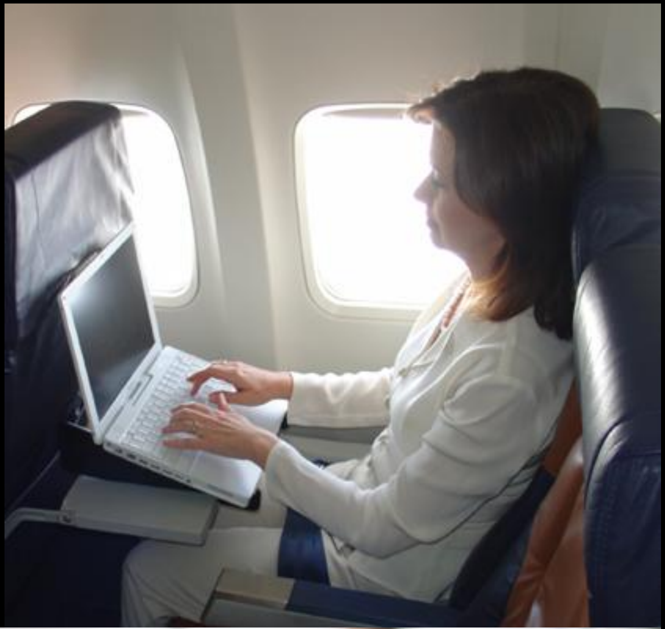
- The confidentiality
- The integrity
- The availability

It’s hard to protect that which we have no idea as to its whereabouts

So, where is our data today?

On any device…

Any place...



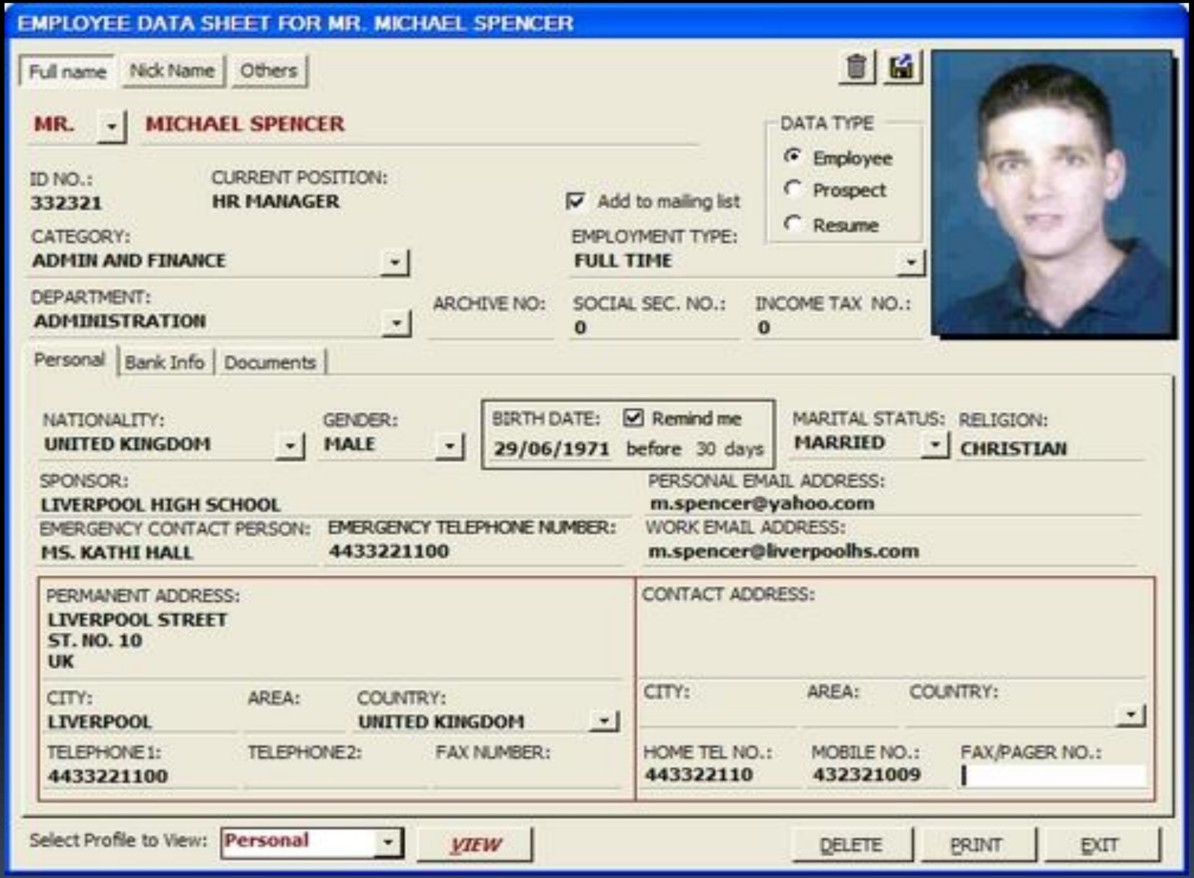
Any time...

Mobile Apps

Your apps

CA Resident's Data

CA Employee Data



EMPLOYEE DATA SHEET FOR MR. MICHAEL SPENCER

MR. MICHAEL SPENCER

DATA TYPE
● Employee
○ Prospect
○ Resume

ID NO.: 332321

CURRENT POSITION: HR MANAGER

☑ Add to mailing list

CATEGORY: ADMIN AND FINANCE

EMPLOYMENT TYPE: FULL TIME

DEPARTMENT: ADMINISTRATION

ARCHIVE NO.:

SOCIAL SEC. NO.: 0

INCOME TAX NO.: 0

NATIONALITY: UNITED KINGDOM

GENDER: MALE

BIRTH DATE: 29/06/1971 ☑ Remind me before 30 days

MARITAL STATUS: MARRIED

RELIGION: CHRISTIAN

SPONSOR: LIVERPOOL HIGH SCHOOL

PERSONAL EMAIL ADDRESS: m.spencer@yahoo.com

EMERGENCY CONTACT PERSON: MS. KATHI HALL

EMERGENCY TELEPHONE NUMBER: 4433221100

WORK EMAIL ADDRESS: m.spencer@liverpoolhs.com

PERMANENT ADDRESS:
LIVERPOOL STREET
ST. NO. 10
UK

CITY: LIVERPOOL

AREA:

COUNTRY: UNITED KINGDOM

TELEPHONE1: 4433221100

TELEPHONE2:

FAX NUMBER:

CONTACT ADDRESS:

CITY:

AREA:

COUNTRY:

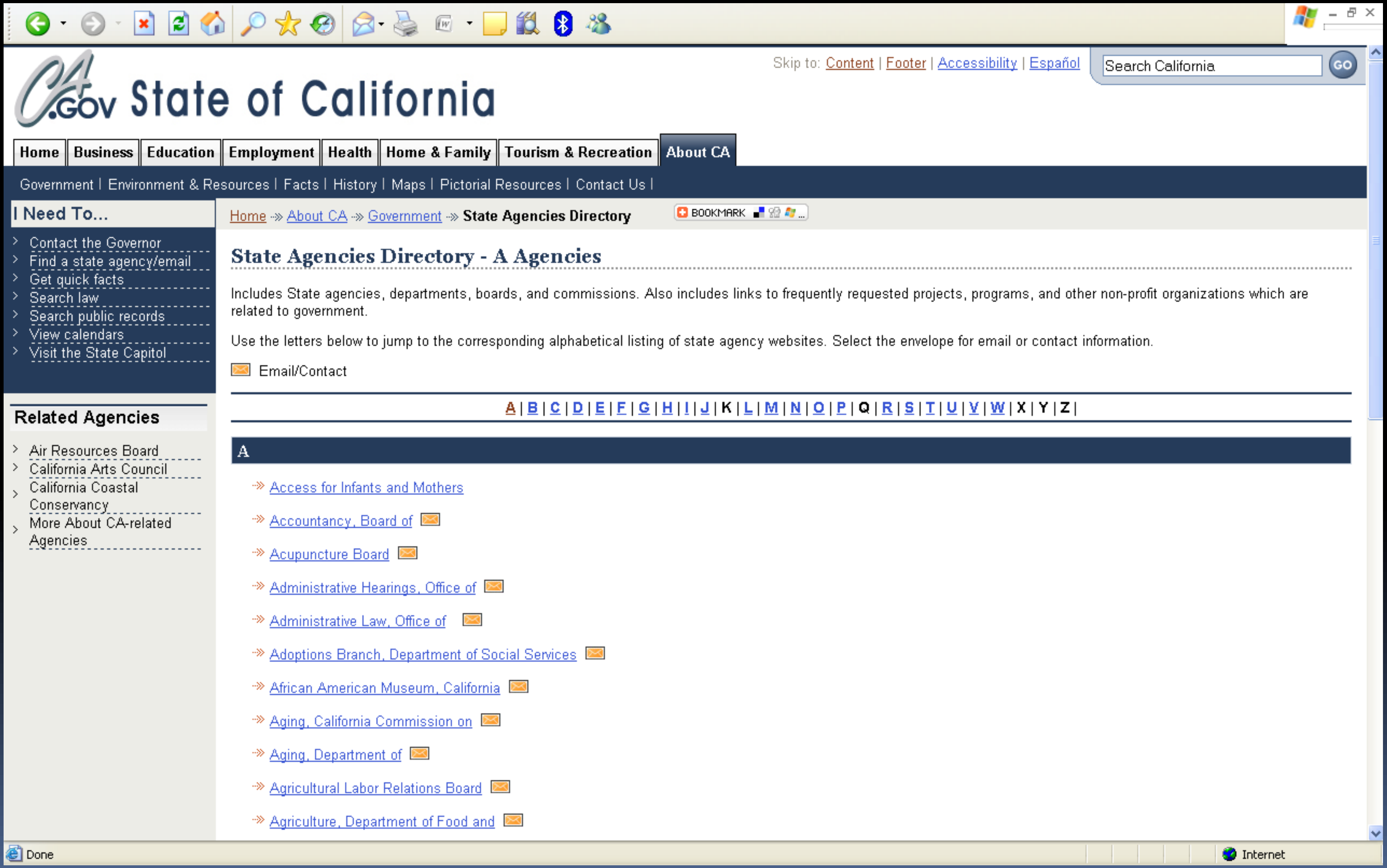
HOME TEL NO.: 443322110

MOBILE NO.: 432321009

FAX/PAGER NO.:

Select Profile to View: Personal

State Agency Data


Skip to: Content | Footer | Accessibility | Español
Search California
GO
State of California
Home
Business
Education
Employment
Health
Home & Family
Tourism & Recreation
About CA
Government | Environment & Resources | Facts | History | Maps | Pictorial Resources | Contact Us |
BOOKMARK
Done
Internet

I Need To...

- Contact the Governor
- Find a state agency/email
- Get quick facts
- Search law
- Search public records
- View calendars
- Visit the State Capitol

Related Agencies

- Air Resources Board
- California Arts Council
- California Coastal Conservancy
- More About CA-related Agencies

Home » About CA » Government » State Agencies Directory

State Agencies Directory - A Agencies

Includes State agencies, departments, boards, and commissions. Also includes links to frequently requested projects, programs, and other non-profit organizations which are related to government.

Use the letters below to jump to the corresponding alphabetical listing of state agency websites. Select the envelope for email or contact information.

✉ Email/Contact

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

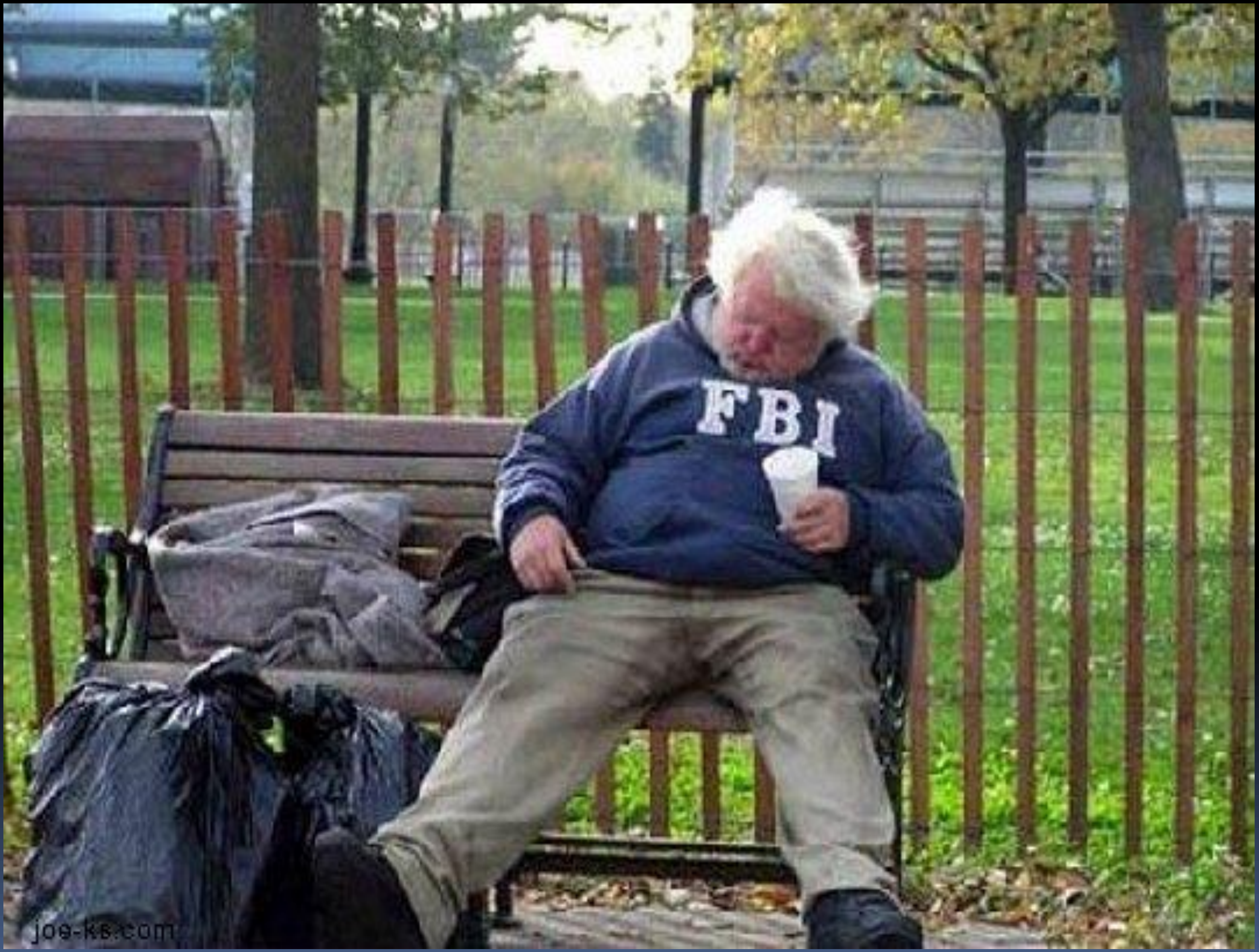
A

- Access for Infants and Mothers
- Accountancy, Board of ✉
- Acupuncture Board ✉
- Administrative Hearings, Office of ✉
- Administrative Law, Office of ✉
- Adoptions Branch, Department of Social Services ✉
- African American Museum, California ✉
- Aging, California Commission on ✉
- Aging, Department of ✉
- Agricultural Labor Relations Board ✉
- Agriculture, Department of Food and ✉

Today, it’s about mobility…

- In the past few years we shifted our lives to the PC and the Internet
- Now, it’s all about being mobile
- A PC in your pocket
- California’s mobile work force is growing and expanding globally

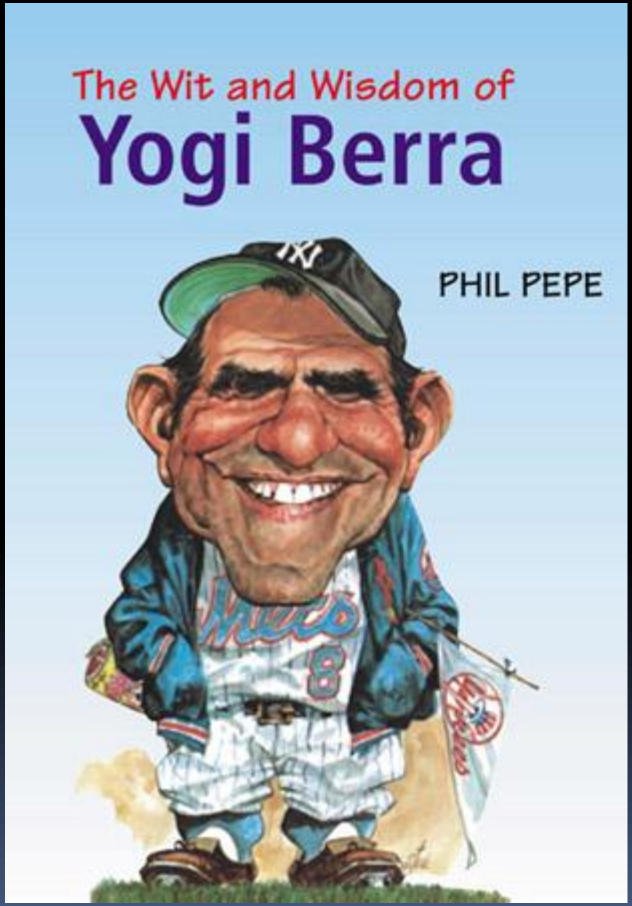
Sleeper Agent



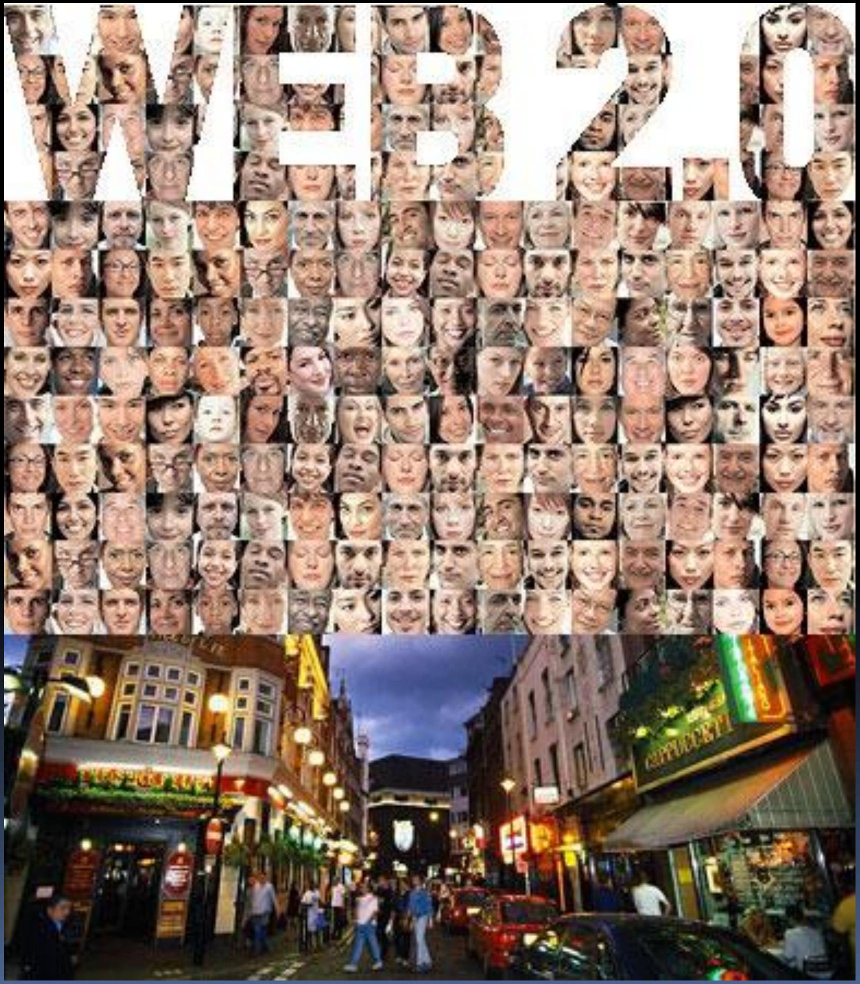
Remember when…

- Security meant having someone who could set a rule on a firewall
- The security officer was at the desk in the lobby
- Browsing was something you did at a Mall
- Podcasting was throwing peas into the wind
- Intrusion prevention was locking your front door
- Identity theft was handing in someone else’s homework
- Data loss was forgetting where you put your car keys
- Those days are gone…

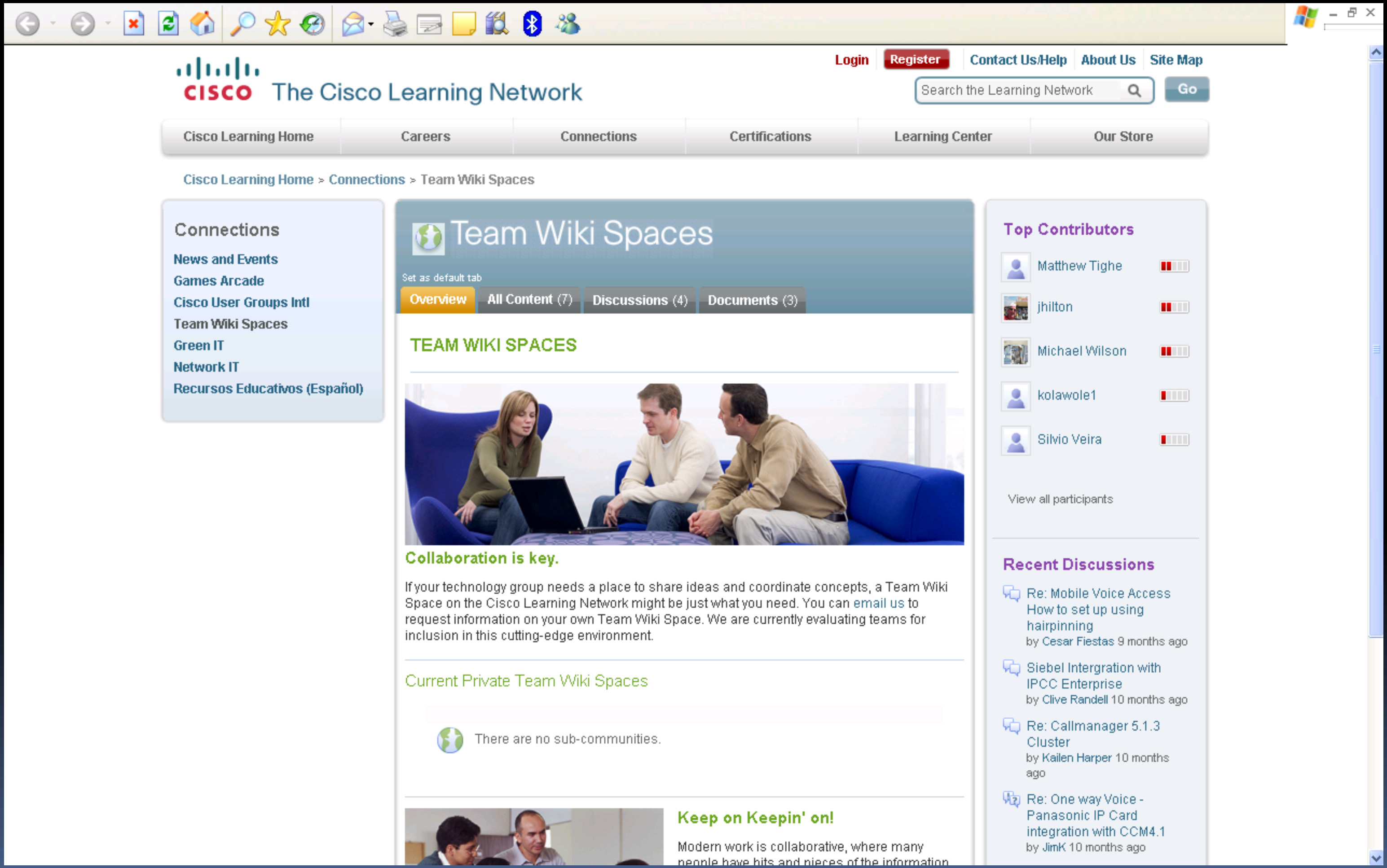
“The future ain’t what it used to be.”



What are we going what are we doing?



Cisco Wikis



Login Register | Contact Us/Help | About Us | Site Map

The Cisco Learning Network

Search the Learning Network | Go

Cisco Learning Home | Careers | Connections | Certifications | Learning Center | Our Store

Cisco Learning Home > Connections > Team Wiki Spaces

Connections

- News and Events
- Games Arcade
- Cisco User Groups Intl
- Team Wiki Spaces
- Green IT
- Network IT
- Recursos Educativos (Español)

Team Wiki Spaces

Set as default tab

Overview | All Content (7) | Discussions (4) | Documents (3)

TEAM WIKI SPACES

Collaboration is key.

If your technology group needs a place to share ideas and coordinate concepts, a Team Wiki Space on the Cisco Learning Network might be just what you need. You can email us to request information on your own Team Wiki Space. We are currently evaluating teams for inclusion in this cutting-edge environment.

Current Private Team Wiki Spaces

There are no sub-communities.

Keep on Keepin' on!

Modern work is collaborative, where many people have bits and pieces of the information

Top Contributors

- Matthew Tighe
- jhilton
- Michael Wilson
- kolawole1
- Silvio Veira

View all participants

Recent Discussions

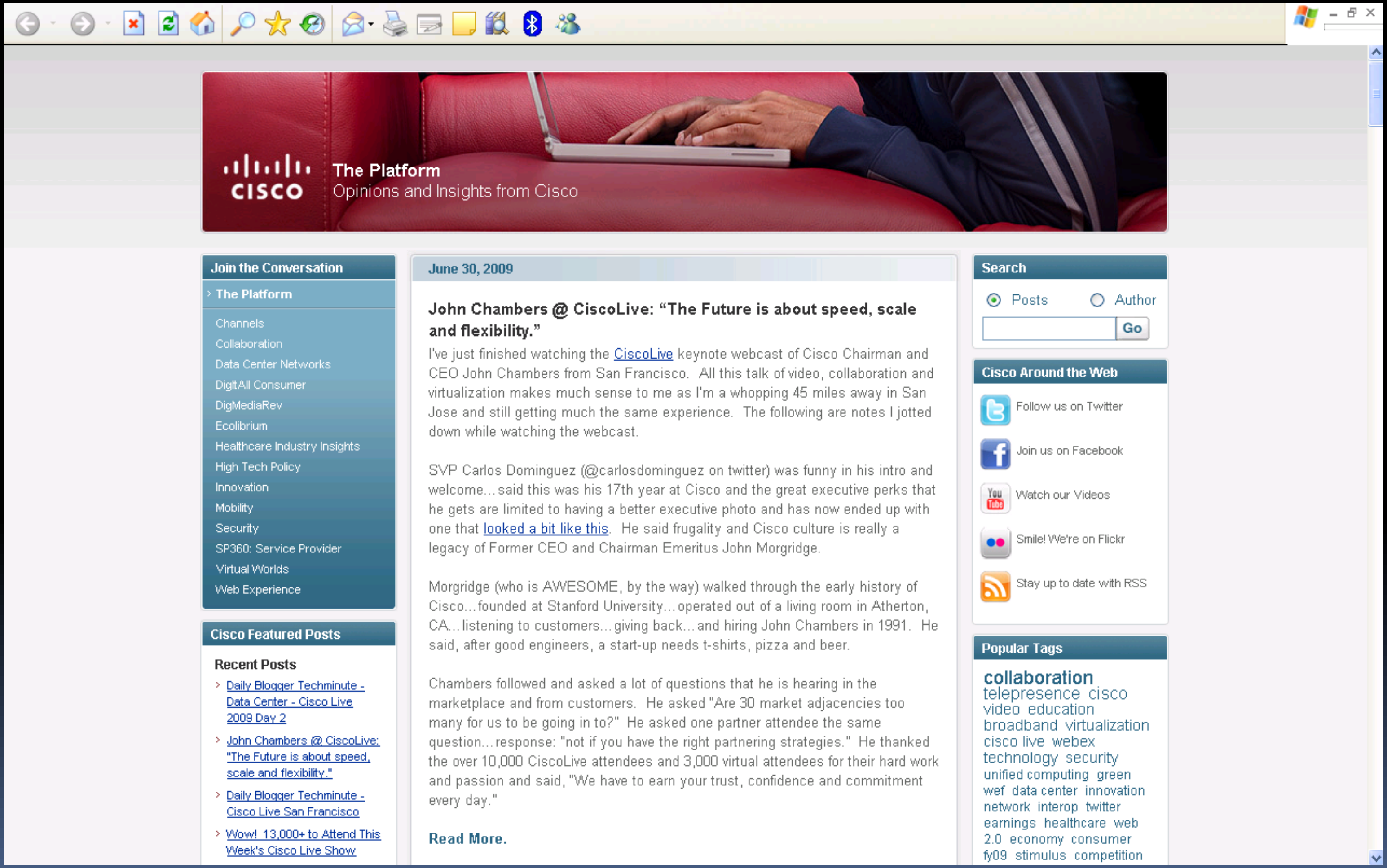
Re: Mobile Voice Access How to set up using hairpinning
by Cesar Fiestas 9 months ago

Siebel Intergration with IPCC Enterprise
by Clive Randell 10 months ago

Re: Callmanager 5.1.3 Cluster
by Kailen Harper 10 months ago

Re: One way Voice - Panasonic IP Card integration with CCM4.1
by JimK 10 months ago

Cisco Blogs



The Platform
Opinions and Insights from Cisco

Join the Conversation

› The Platform

Channels
Collaboration
Data Center Networks
DigitAll Consumer
DigMediaRev
Ecolibrium
Healthcare Industry Insights
High Tech Policy
Innovation
Mobility
Security
SP360: Service Provider
Virtual Worlds
Web Experience

Cisco Featured Posts

Recent Posts

- Daily Blogger Techminute - Data Center - Cisco Live 2009 Day 2
- John Chambers @ CiscoLive: "The Future is about speed, scale and flexibility."
- Daily Blogger Techminute - Cisco Live San Francisco
- Wow! 13,000+ to Attend This Week's Cisco Live Show

June 30, 2009

John Chambers @ CiscoLive: "The Future is about speed, scale and flexibility."

I've just finished watching the CiscoLive keynote webcast of Cisco Chairman and CEO John Chambers from San Francisco. All this talk of video, collaboration and virtualization makes much sense to me as I'm a whopping 45 miles away in San Jose and still getting much the same experience. The following are notes I jotted down while watching the webcast.

SVP Carlos Dominguez (@carlosdominguez on twitter) was funny in his intro and welcome...said this was his 17th year at Cisco and the great executive perks that he gets are limited to having a better executive photo and has now ended up with one that looked a bit like this. He said frugality and Cisco culture is really a legacy of Former CEO and Chairman Emeritus John Morgridge.

Morgridge (who is AWESOME, by the way) walked through the early history of Cisco...founded at Stanford University...operated out of a living room in Atherton, CA...listening to customers...giving back...and hiring John Chambers in 1991. He said, after good engineers, a start-up needs t-shirts, pizza and beer.

Chambers followed and asked a lot of questions that he is hearing in the marketplace and from customers. He asked "Are 30 market adjacencies too many for us to be going in to?" He asked one partner attendee the same question...response: "not if you have the right partnering strategies." He thanked the over 10,000 CiscoLive attendees and 3,000 virtual attendees for their hard work and passion and said, "We have to earn your trust, confidence and commitment every day."

Read More.

Search

● Posts ○ Author

Go

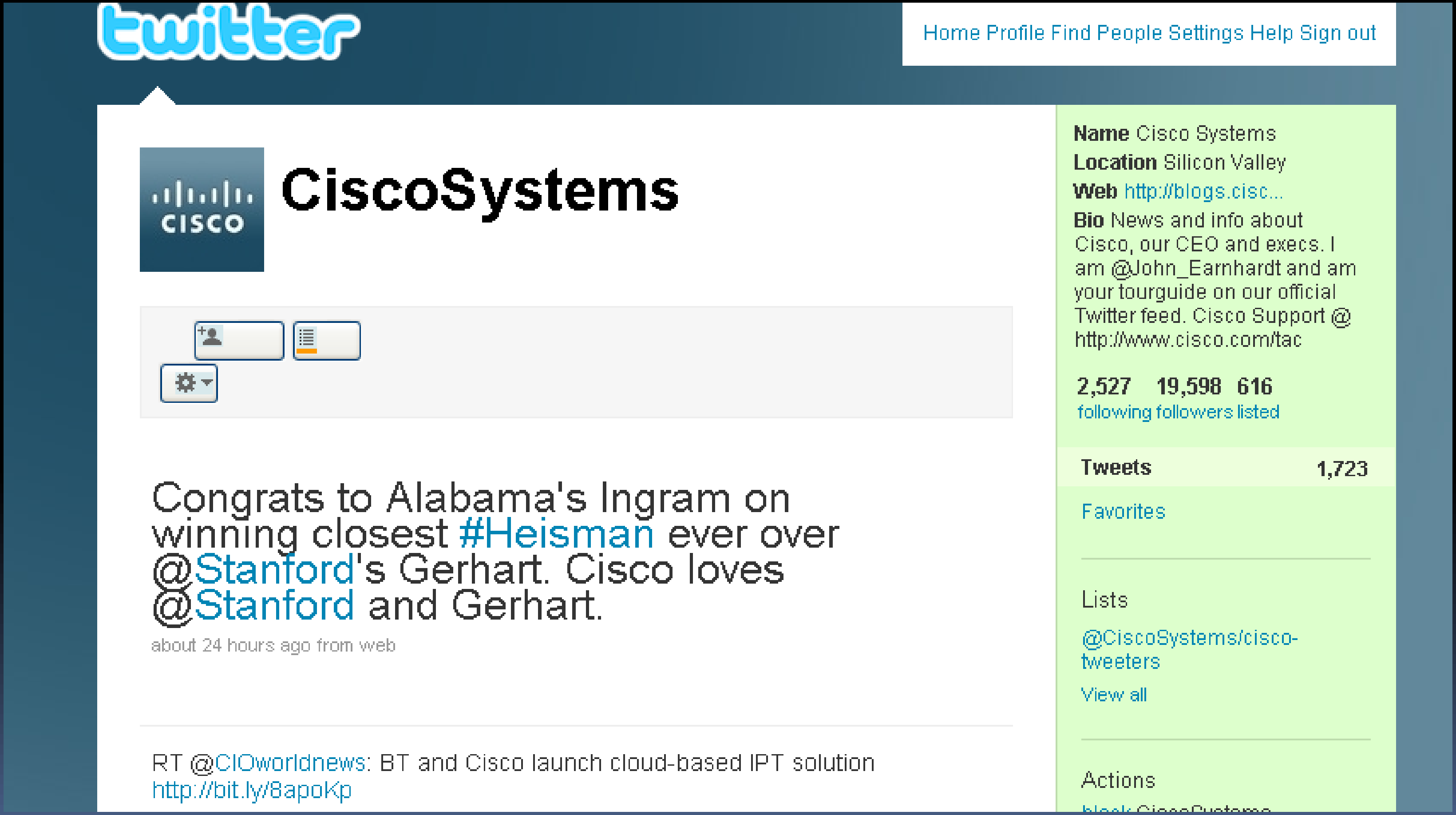
Cisco Around the Web

Follow us on Twitter
Join us on Facebook
Watch our Videos
Smile! We're on Flickr
Stay up to date with RSS

Popular Tags

collaboration telepresence cisco video education broadband virtualization cisco live webex technology security unified computing green wef data center innovation network interop twitter earnings healthcare web 2.0 economy consumer fy09 stimulus competition

Cisco on Twitter



CiscoSystems

Congrats to Alabama's Ingram on winning closest #Heisman ever over @Stanford's Gerhart. Cisco loves @Stanford and Gerhart.

about 24 hours ago from web

RT @CIOworldnews: BT and Cisco launch cloud-based IPT solution http://bit.ly/8apoKp

Name Cisco Systems
Location Silicon Valley
Web http://blogs.cisc...
Bio News and info about Cisco, our CEO and execs. I am @John_Earnhardt and am your tourguide on our official Twitter feed. Cisco Support @ http://www.cisco.com/tac

2,527	19,598	616
following	followers	listed

Tweets 1,723

Favorites

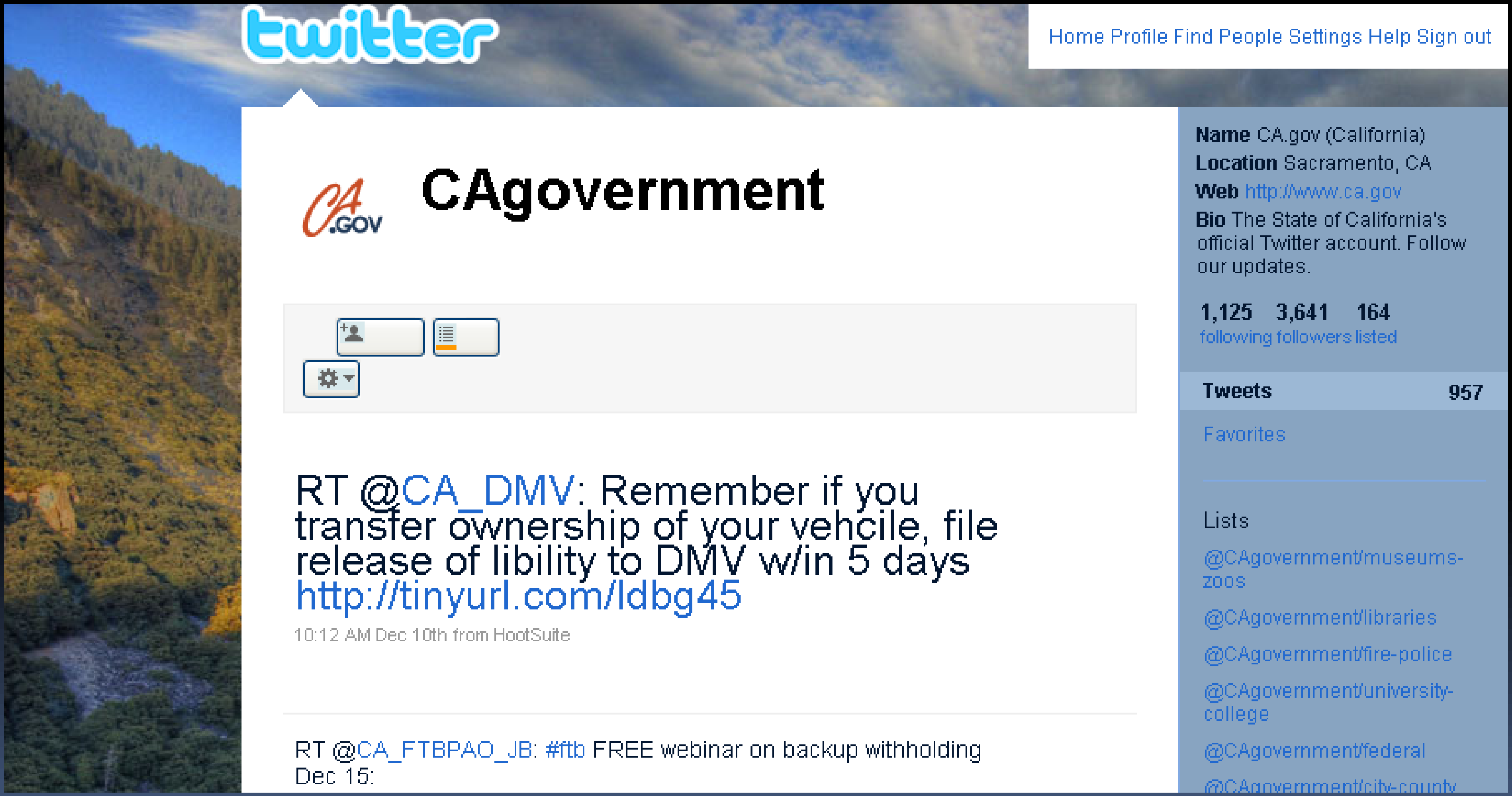
Lists

@CiscoSystems/cisco-tweeters

View all

Actions

CA on Twitter



CAgovernment

RT @CA_DMV: Remember if you transfer ownership of your vehcile, file release of libility to DMV w/in 5 days http://tinyurl.com/ldbg45

10:12 AM Dec 10th from HootSuite

RT @CA_FTBPAO_JB: #ftb FREE webinar on backup withholding Dec 15:

Name CA.gov (California)
Location Sacramento, CA
Web http://www.ca.gov
Bio The State of California's official Twitter account. Follow our updates.

1,125	3,641	164
following	followers	listed

Tweets 957

Favorites

Lists

@CAgovernment/museums-zoos

@CAgovernment/libraries

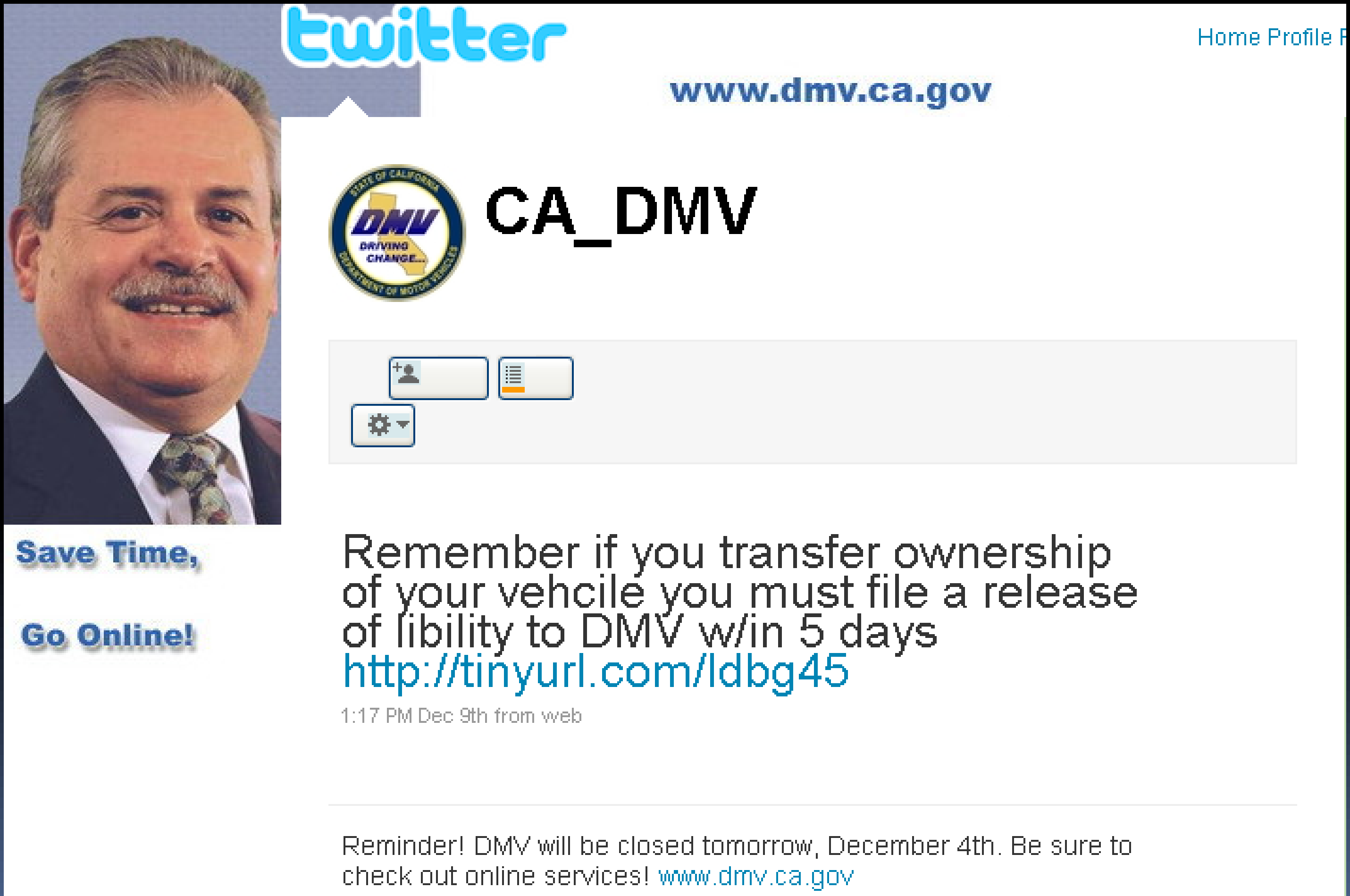
@CAgovernment/fire-police

@CAgovernment/university-college

@CAgovernment/federal

@CAgovernment/city-county

Explaining Services



CA_DMV

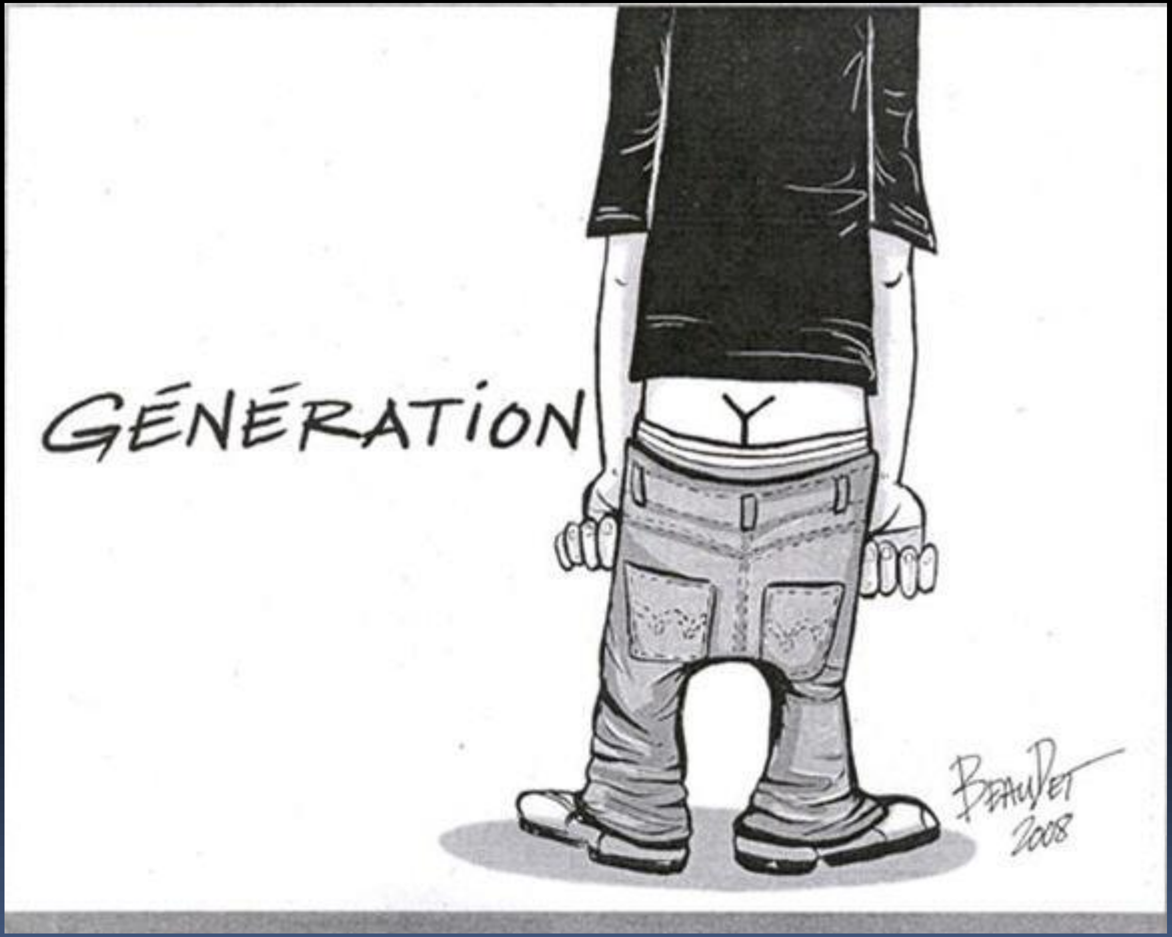
Remember if you transfer ownership of your vehcile you must file a release of libility to DMV w/in 5 days http://tinyurl.com/ldbg45

1:17 PM Dec 9th from web

Reminder! DMV will be closed tomorrow, December 4th. Be sure to check out online services! www.dmv.ca.gov

Guess who this is…

Yup, Generation Y is on the network – Like it or not, they're here to stay

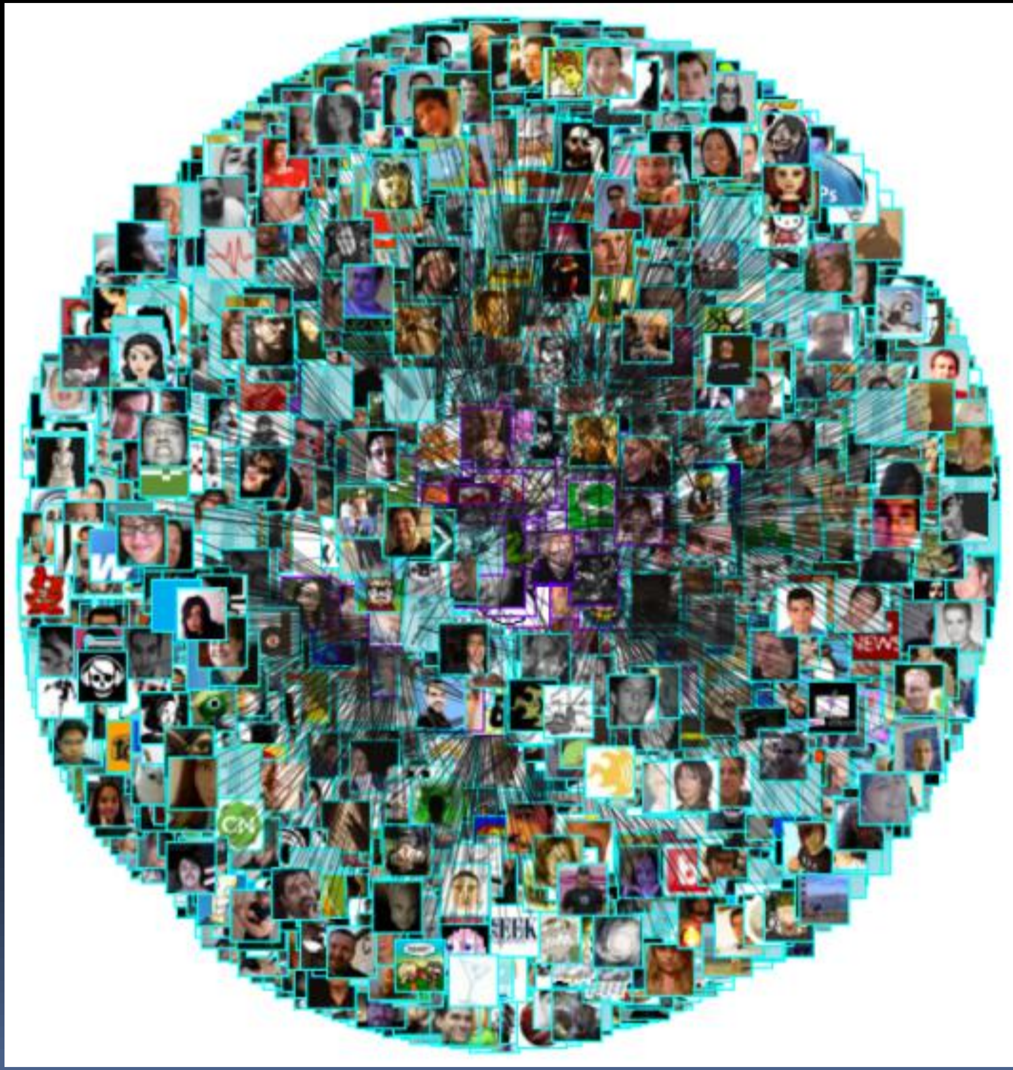


So, where are we going and what are we doing once we get there?

There is a human element to all of this, an element that is more often than not, overlooked…

It’s no longer just close relationships

- State employees, are going places they’ve never gone before and are touching technology daily
- That which they are touching is touching Agency networks as well



With Web 2.0

- A new breed of malware is evolving
- Google Mashups, RSS feeds, search, all of these can be misused by hackers to distribute malware, attack Web surfers and communicate with botnets

What are the Risks with Web 2.0?

- Social networking is the norm today
- It marks the global trend of seeking friendships or relationships online
- Gradually getting into business life, where networks are used for boosting interactions with customers, banks, brokers and others
- Enhancing communication with colleagues, as well as being a platform for promotion of services and promotions

Risk – it's everywhere

- And no one knows that better than IT security professionals
- Disgruntled employees, fired employees, clueless employees who succumb to social engineering, passwords left on Post-it notes, wide-open instant messaging and increasingly powerful hacker tools in the hands of teenagers, Web Mobs and Organized Crime targeting Social Media sites

Objective?

- The key objective, of course, is to recognize risk, safeguard your reputation and not reveal sensitive or confidential information that may prove harmful to the business

So, what do we have to do?

- Create a Human Firewall

The Human Firewall – an invaluable tool

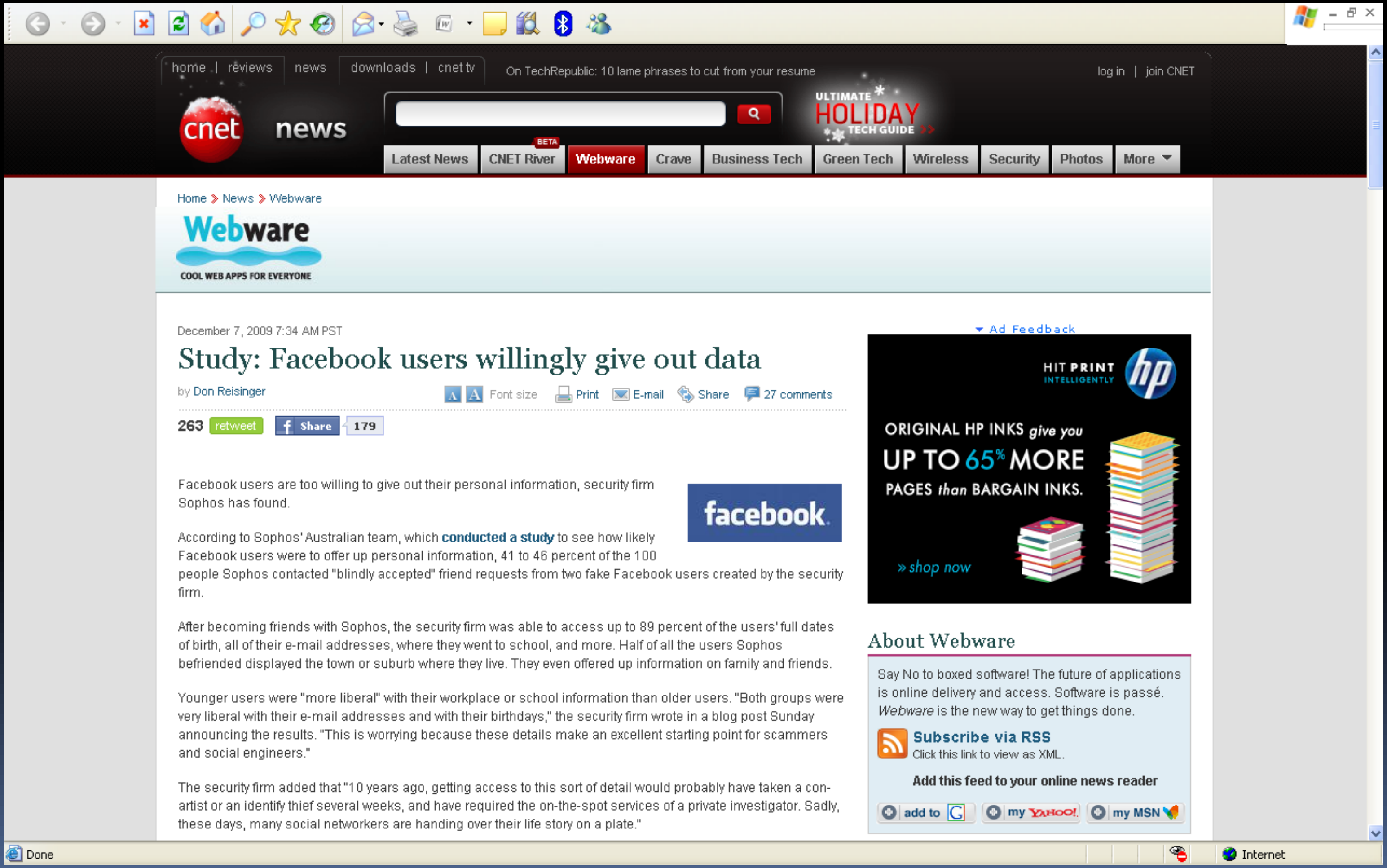
- A good *human firewall employee* is one who filters good security practices and rejects any others—much like a network firewall only allows authorized traffic and rejects any other
- The only way to build a good human firewall is to raise people's awareness; to teach them good habits, to make them recognize bad practices and change them into good practices
- Your cyber security is only as good as the people who manage and those who use it

So Patrick, why do we really need that Human Firewall?

Because, ‘Friend’ has become a verb

- Social media users believe there is protection in being part of a community of people they know
- Criminals are happy to prove this notion wrong

My new friends…



home | reviews | news | downloads | cnet tv
On TechRepublic: 10 lame phrases to cut from your resume
log in | join CNET
cnet news
ULTIMATE HOLIDAY TECH GUIDE
Latest News
CNET River BETA
Webware
Crave
Business Tech
Green Tech
Wireless
Security
Photos
More
Done
Internet

Home > News > Webware

Webware
COOL WEB APPS FOR EVERYONE

December 7, 2009 7:34 AM PST

Study: Facebook users willingly give out data

by Don Reisinger

A A Font size | Print | E-mail | Share | 27 comments

263 retweet | Share 179

Facebook users are too willing to give out their personal information, security firm Sophos has found.

According to Sophos' Australian team, which **conducted a study** to see how likely Facebook users were to offer up personal information, 41 to 46 percent of the 100 people Sophos contacted "blindly accepted" friend requests from two fake Facebook users created by the security firm.

After becoming friends with Sophos, the security firm was able to access up to 89 percent of the users' full dates of birth, all of their e-mail addresses, where they went to school, and more. Half of all the users Sophos befriended displayed the town or suburb where they live. They even offered up information on family and friends.

Younger users were "more liberal" with their workplace or school information than older users. "Both groups were very liberal with their e-mail addresses and with their birthdays," the security firm wrote in a blog post Sunday announcing the results. "This is worrying because these details make an excellent starting point for scammers and social engineers."

The security firm added that "10 years ago, getting access to this sort of detail would probably have taken a con-artist or an identify thief several weeks, and have required the on-the-spot services of a private investigator. Sadly, these days, many social networkers are handing over their life story on a plate."

About Webware

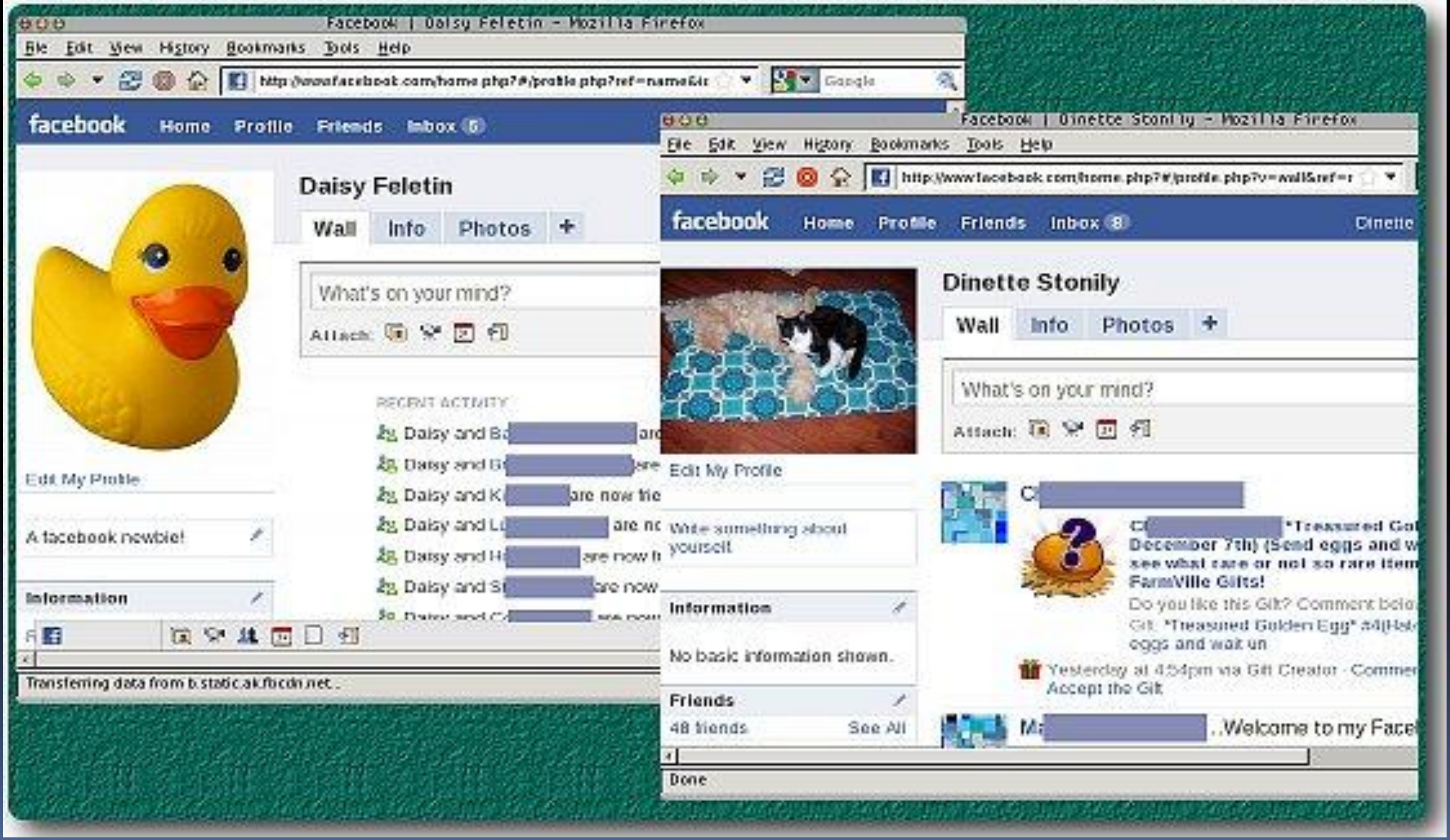
Say No to boxed software! The future of applications is online delivery and access. Software is passé. *Webware* is the new way to get things done.

Subscribe via RSS
Click this link to view as XML.

Add this feed to your online news reader

add to G | my YAHOO! | my MSN

46% accepted and gave full access


Facebook | Daisy Feletin - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.facebook.com/home.php?#/profile.php?ref=name&ic
Google
facebook
Home
Profile
Friends
Inbox 6
Wall
Info
Photos
+
Attach:
Edit My Profile
Information
Facebook | Dinette Stonily - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.facebook.com/home.php?#/profile.php?v=wall&ref=r
facebook
Home
Profile
Friends
Inbox 8
Dinette
Wall
Info
Photos
+
Attach:
Edit My Profile
Information
Friends
See All
Done

Daisy Feletin

What's on your mind?

RECENT ACTIVITY

Daisy and Ba [redacted] are

Daisy and G [redacted] were

Daisy and K [redacted] are now frie

Daisy and L [redacted] are no

Daisy and H [redacted] are now fr

Daisy and S [redacted] are now

Daisy and C [redacted] are now

A facebook newbie!

Transferring data from b.static.ak.fbcdn.net...

Dinette Stonily

What's on your mind?

Write something about yourself.

No basic information shown.

48 friends

C [redacted]

C [redacted] *Treasured Gol December 7th) (Send eggs and w see what rare or not so rare item FarmVille Gifts!

Do you like this Gift? Comment belo Gift. *Treasured Golden Egg* #4(Help eggs and wait un

Yesterday at 4:54pm via Gift Creator · Commen Accept the Gift

M [redacted] ..Welcome to my Face

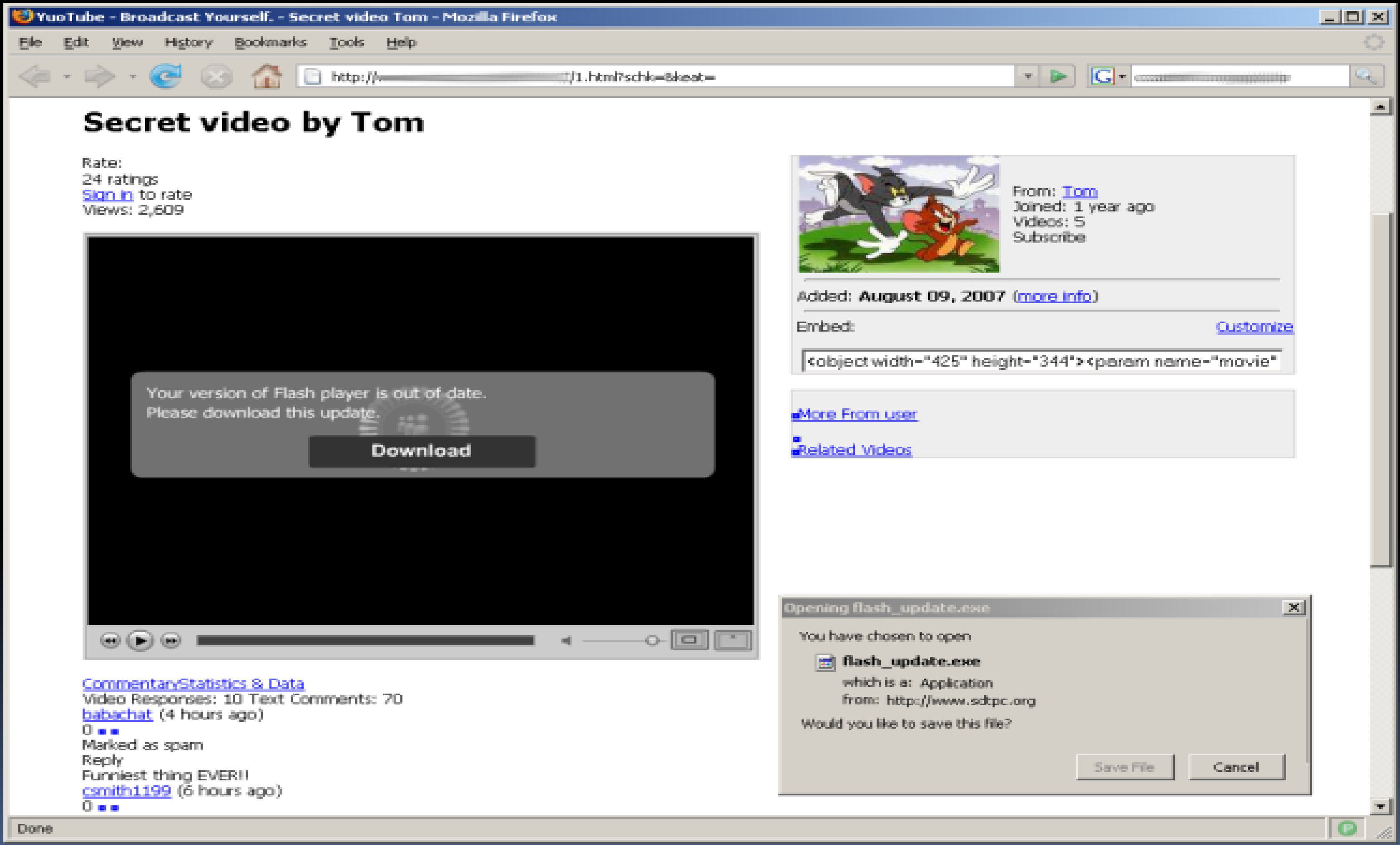
The “herd” mentality

- The threats and security issues that come with social media aren’t usually caused by vulnerabilities in software
- More commonly, these threats originate from individuals who place an unwarranted amount of “transitive trust” in the safety of these communities

Trust?

- Users will trust something or someone because a user they know has also expressed trust in that person or subject
- We trust because we are curious and curiosity…

Curious? This is why! Out of date???



YuoTube - Broadcast Yourself. - Secret video Tom - Mozilla Firefox

http://[redacted]/1.html?schk=&keat=

[redacted]

Secret video by Tom

Rate:
24 ratings
Sign in to rate
Views: 2,609

Your version of Flash player is out of date.
Please download this update.

From: Tom
Joined: 1 year ago
Videos: 5
Subscribe

Added: August 09, 2007 (more info)

Embed: Customize

```
<object width="425" height="344"><param name="movie"
```

More From user

Related Videos

CommentaryStatistics & Data
Video Responses: 10 Text Comments: 70
babachat (4 hours ago)
0
Marked as spam
Reply
Funniest thing EVER!!
csmith1199 (6 hours ago)
0

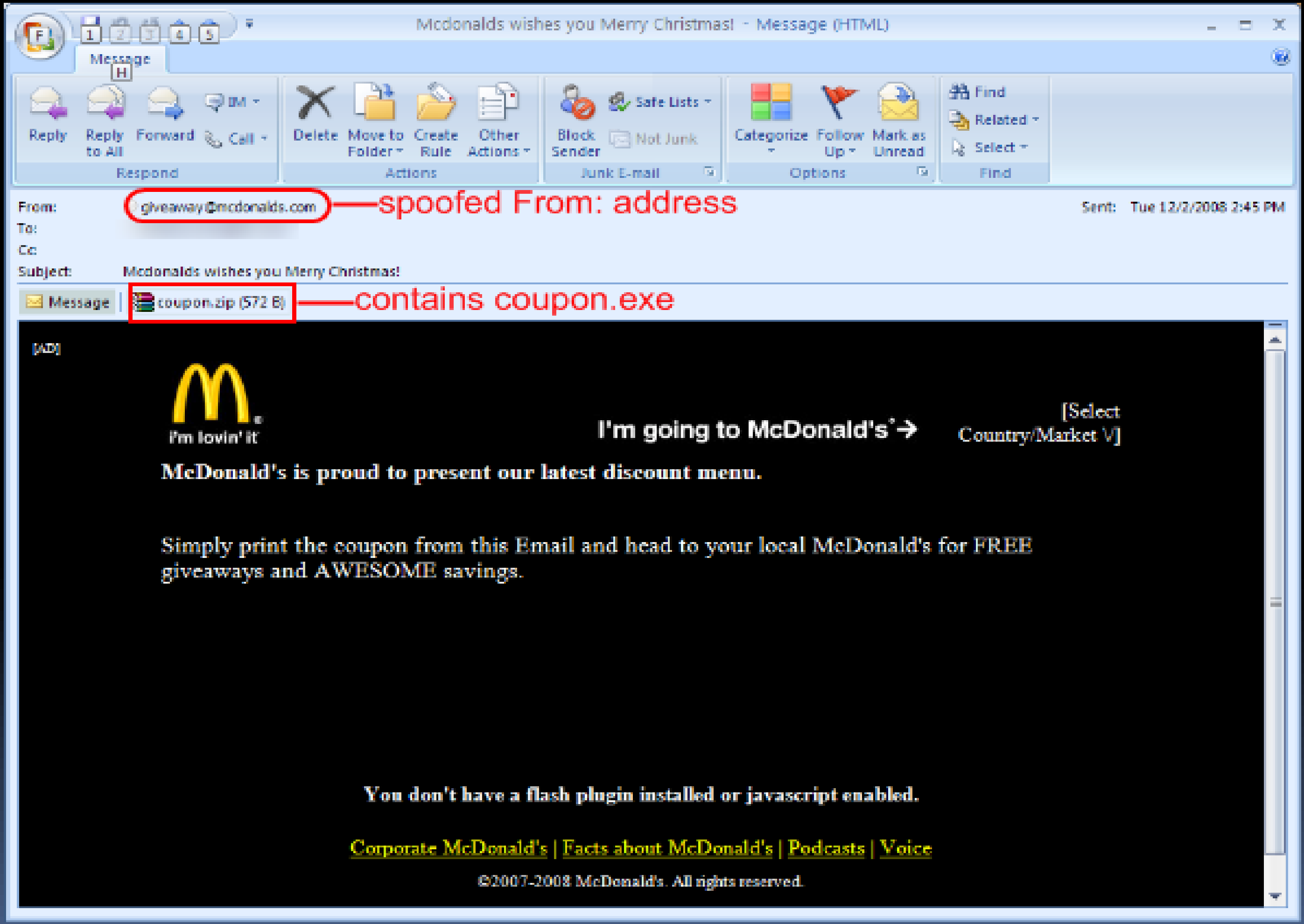
Opening flash_update.exe

You have chosen to open

flash_update.exe
which is a: Application
from: http://www.sdtpc.org

Would you like to save this file?

Or a Big Mac!



From: giveaway@mcdonalds.com —spoofed From: address

To:

Cc:

Subject: Mcdonalds wishes you Merry Christmas!

Sent: Tue 12/2/2008 2:45 PM

Message | coupon.zip (572 B) —contains coupon.exe

[AD]

I'm lovin' it

I'm going to McDonald's →

[Select Country/Market V]

McDonald's is proud to present our latest discount menu.

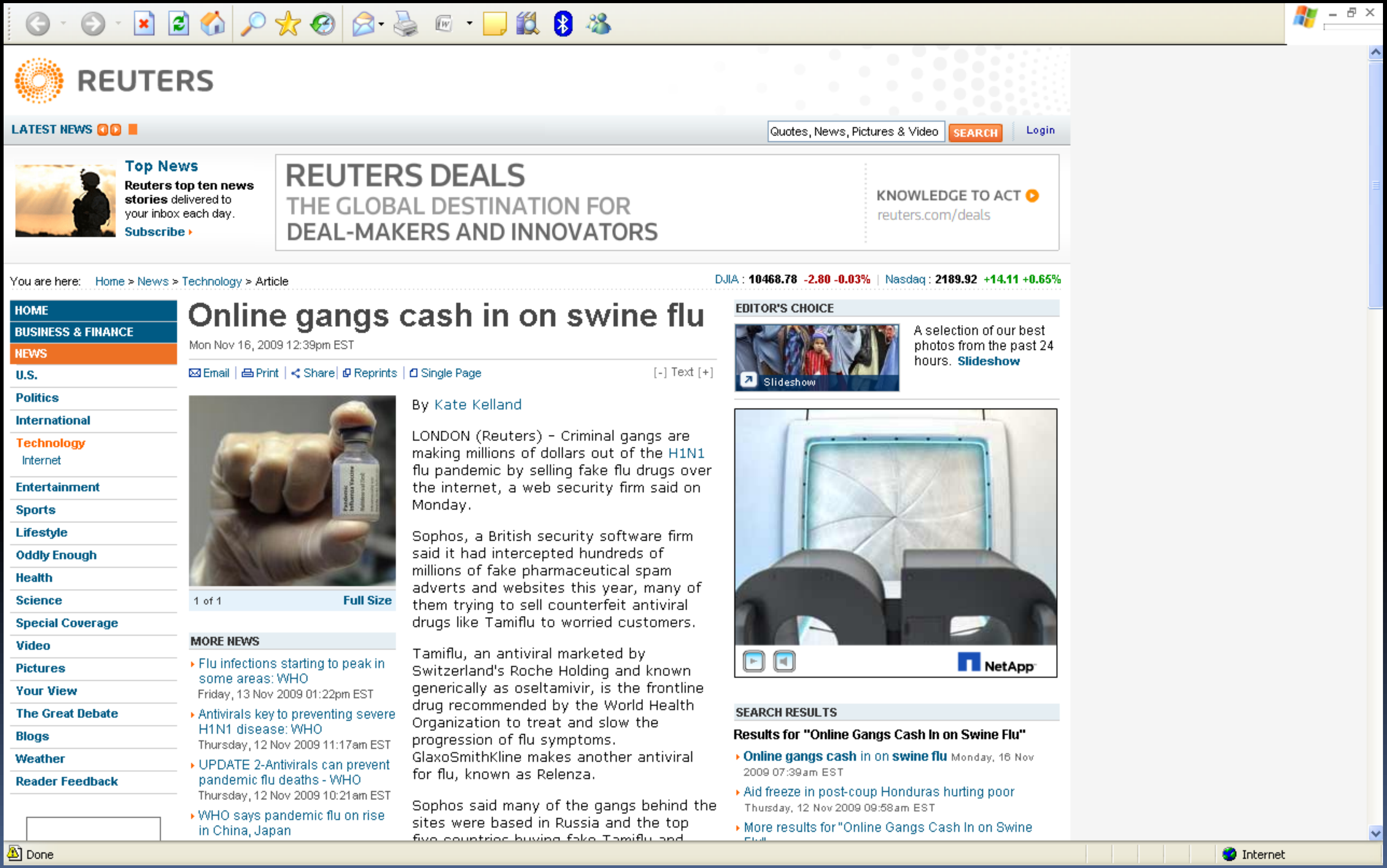
Simply print the coupon from this Email and head to your local McDonald's for FREE giveaways and AWESOME savings.

You don't have a flash plugin installed or javascript enabled.

Corporate McDonald's | Facts about McDonald's | Podcasts | Voice

©2007-2008 McDonald's. All rights reserved.

Or bogus health information



You are here: Home > News > Technology > Article

DJIA : 10468.78 -2.80 -0.03% | Nasdaq : 2189.92 +14.11 +0.65%

Online gangs cash in on swine flu

Mon Nov 16, 2009 12:39pm EST

By Kate Kelland

LONDON (Reuters) - Criminal gangs are making millions of dollars out of the H1N1 flu pandemic by selling fake flu drugs over the internet, a web security firm said on Monday.

Sophos, a British security software firm said it had intercepted hundreds of millions of fake pharmaceutical spam adverts and websites this year, many of them trying to sell counterfeit antiviral drugs like Tamiflu to worried customers.

Tamiflu, an antiviral marketed by Switzerland's Roche Holding and known generically as oseltamivir, is the frontline drug recommended by the World Health Organization to treat and slow the progression of flu symptoms. GlaxoSmithKline makes another antiviral for flu, known as Relenza.

Sophos said many of the gangs behind the sites were based in Russia and the top five countries buying fake Tamiflu and

MORE NEWS

- Flu infections starting to peak in some areas: WHO
  Friday, 13 Nov 2009 01:22pm EST
- Antivirals key to preventing severe H1N1 disease: WHO
  Thursday, 12 Nov 2009 11:17am EST
- UPDATE 2-Antivirals can prevent pandemic flu deaths - WHO
  Thursday, 12 Nov 2009 10:21am EST
- WHO says pandemic flu on rise in China, Japan

EDITOR'S CHOICE

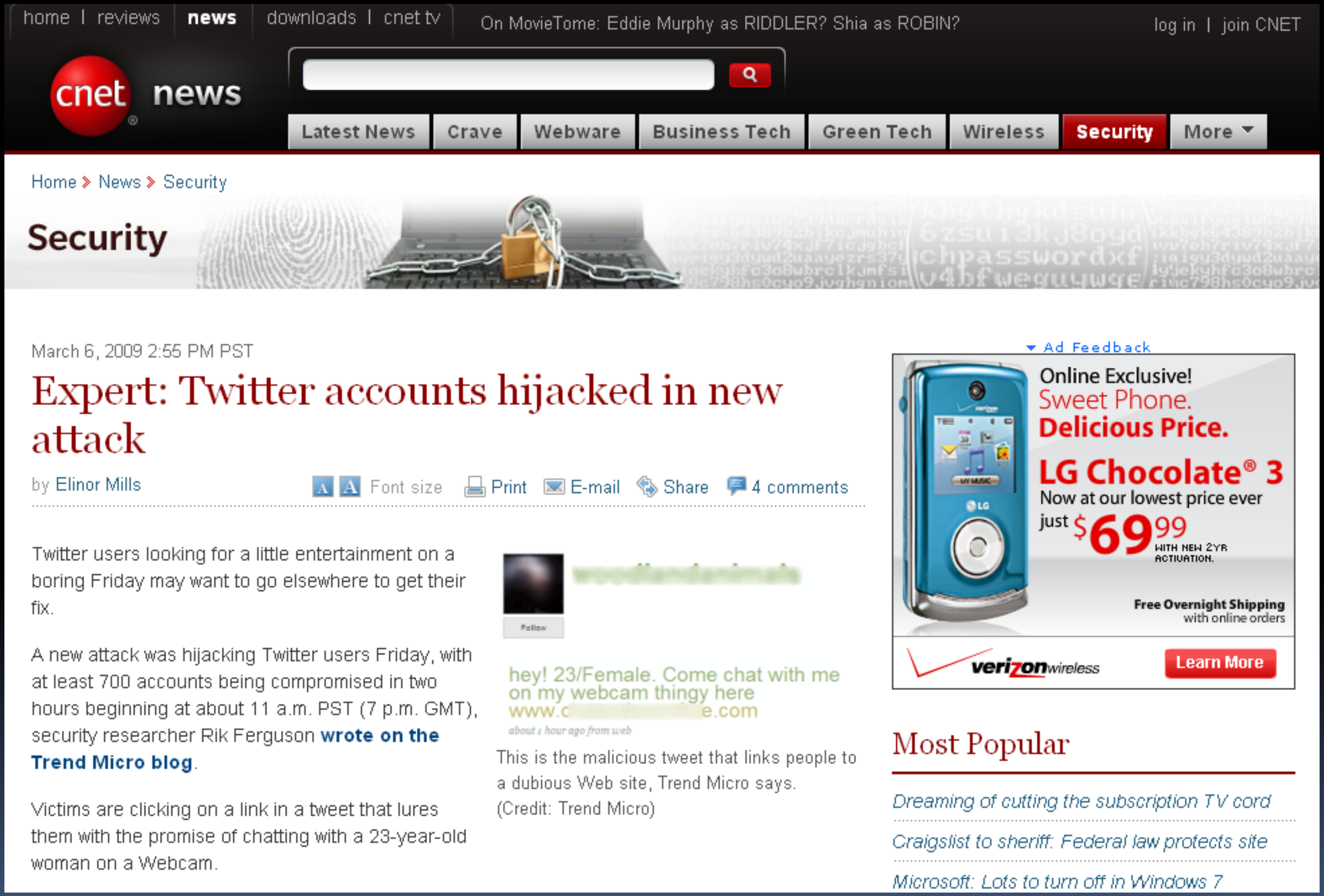
A selection of our best photos from the past 24 hours. Slideshow

SEARCH RESULTS

Results for "Online Gangs Cash In on Swine Flu"

- Online gangs cash in on swine flu Monday, 16 Nov 2009 07:39am EST
- Aid freeze in post-coup Honduras hurting poor
  Thursday, 12 Nov 2009 09:58am EST
- More results for "Online Gangs Cash In on Swine Flu"

Do you Tweet?



March 6, 2009 2:55 PM PST

Expert: Twitter accounts hijacked in new attack

by Elinor Mills

Twitter users looking for a little entertainment on a boring Friday may want to go elsewhere to get their fix.

A new attack was hijacking Twitter users Friday, with at least 700 accounts being compromised in two hours beginning at about 11 a.m. PST (7 p.m. GMT), security researcher Rik Ferguson **wrote on the Trend Micro blog**.

Victims are clicking on a link in a tweet that lures them with the promise of chatting with a 23-year-old woman on a Webcam.

[redacted]

hey! 23/Female. Come chat with me on my webcam thingy here www.c[redacted]e.com

about 1 hour ago from web

This is the malicious tweet that links people to a dubious Web site, Trend Micro says. (Credit: Trend Micro)

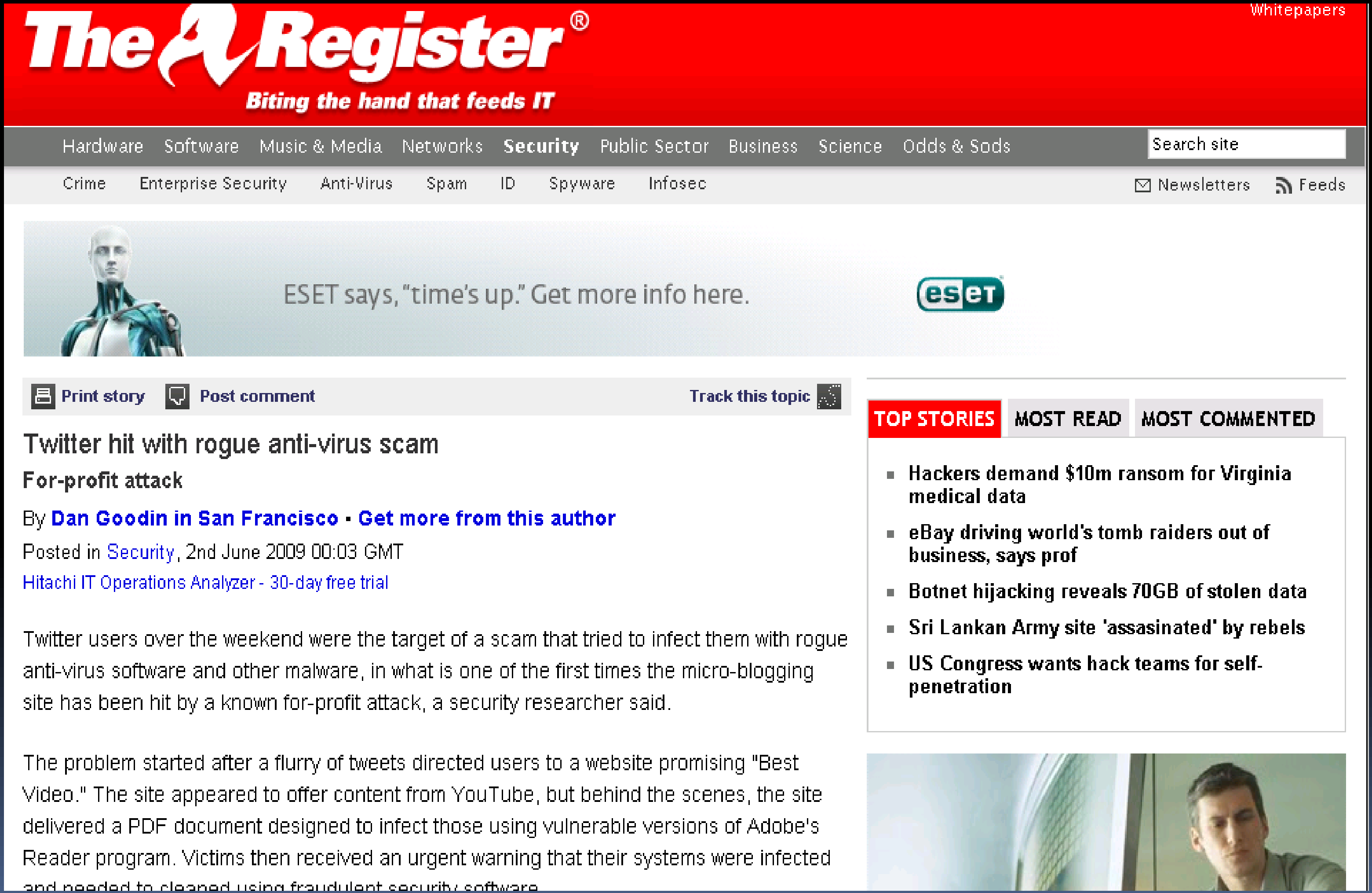
Most Popular

- *Dreaming of cutting the subscription TV cord*
- *Craigslist to sheriff: Federal law protects site*
- *Microsoft: Lots to turn off in Windows 7*

How and why?

- 700 accounts were compromised in two hours
- Victims were clicking on a link in a tweet that lured them with the promise of chatting with a 23-year-old woman on a Webcam
- Uh uh! That’s a no no!

They want to send us somewhere else…



Whitepapers
The Register®
Biting the hand that feeds IT
Hardware Software Music & Media Networks Security Public Sector Business Science Odds & Sods
Search site
Crime Enterprise Security Anti-Virus Spam ID Spyware Infosec
Newsletters
Feeds

Print story
Post comment
Track this topic

Twitter hit with rogue anti-virus scam

For-profit attack

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 2nd June 2009 00:03 GMT

Twitter users over the weekend were the target of a scam that tried to infect them with rogue anti-virus software and other malware, in what is one of the first times the micro-blogging site has been hit by a known for-profit attack, a security researcher said.

The problem started after a flurry of tweets directed users to a website promising "Best Video." The site appeared to offer content from YouTube, but behind the scenes, the site delivered a PDF document designed to infect those using vulnerable versions of Adobe's Reader program. Victims then received an urgent warning that their systems were infected and needed to cleaned using fraudulent security software.

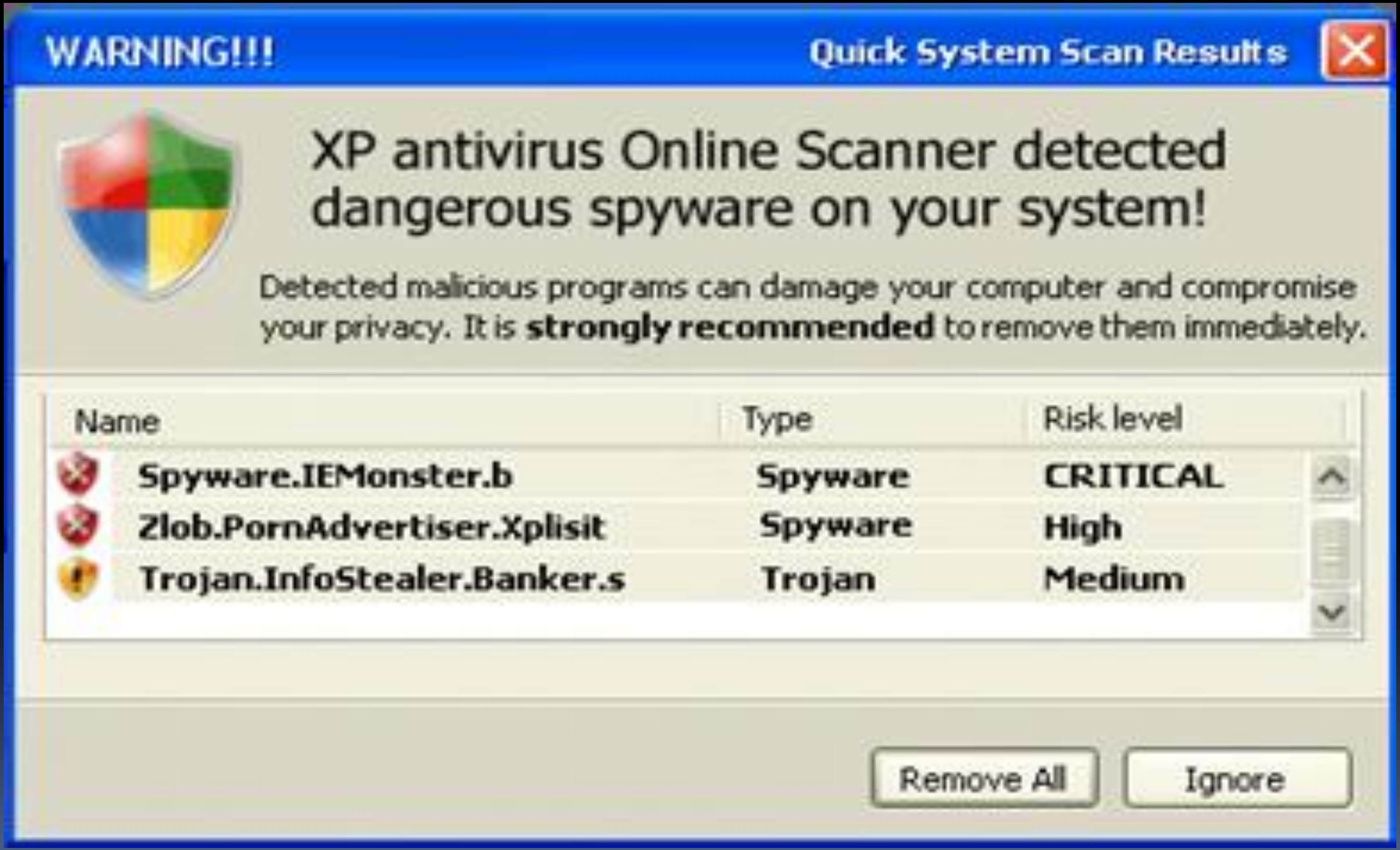
TOP STORIES **MOST READ** **MOST COMMENTED**

- **Hackers demand $10m ransom for Virginia medical data**
- **eBay driving world's tomb raiders out of business, says prof**
- **Botnet hijacking reveals 70GB of stolen data**
- **Sri Lankan Army site 'assasinated' by rebels**
- **US Congress wants hack teams for self-penetration**

Don’t go there!

Stay on the path that you know well!

The unknown… DO NOT TOUCH THIS!!!



WARNING!!!

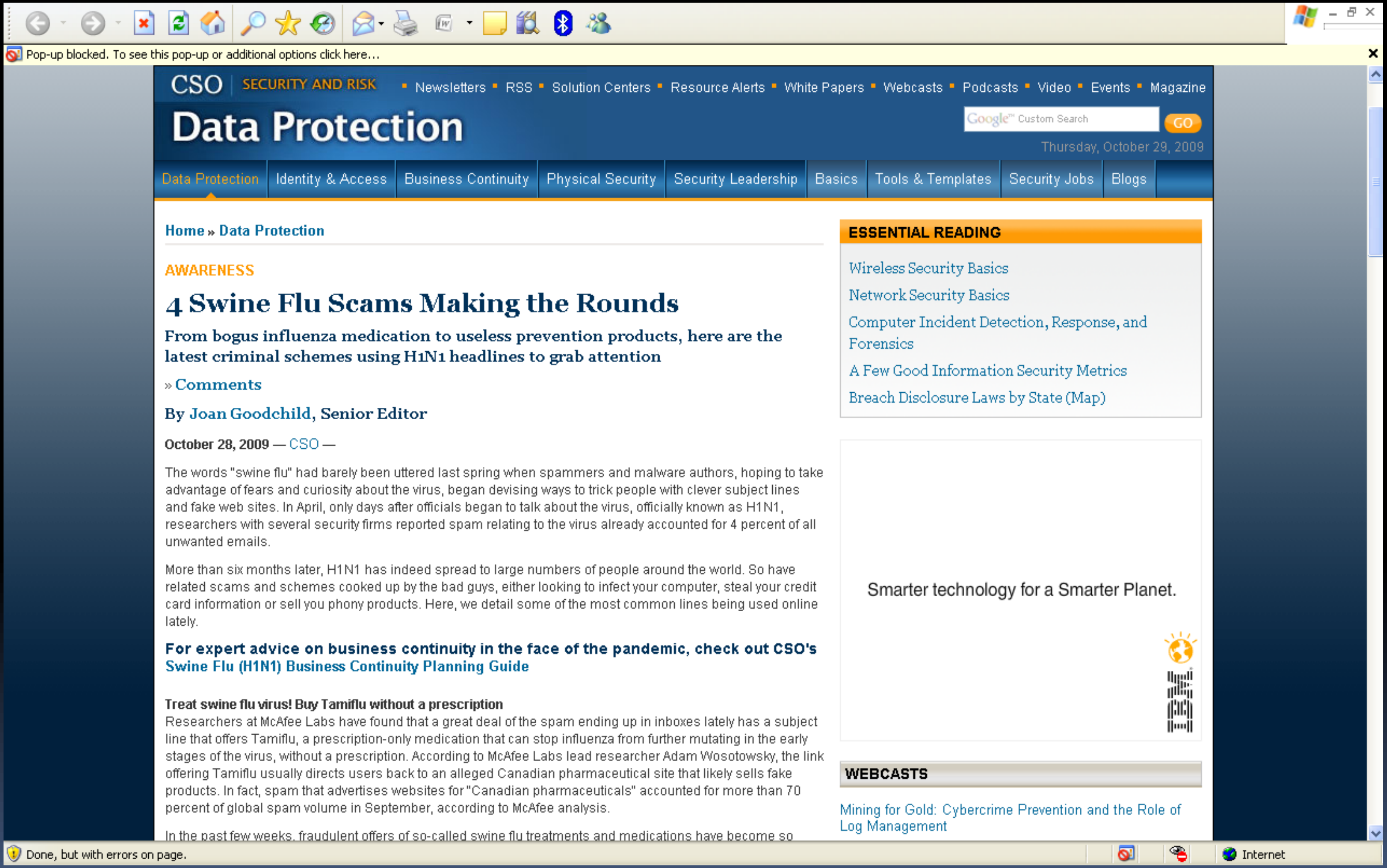
Quick System Scan Results

XP antivirus Online Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplisit	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

They play on our fears



Pop-up blocked. To see this pop-up or additional options click here...

CSO SECURITY AND RISK

Data Protection

Thursday, October 29, 2009

Home » Data Protection

AWARENESS

4 Swine Flu Scams Making the Rounds

From bogus influenza medication to useless prevention products, here are the latest criminal schemes using H1N1 headlines to grab attention

» Comments

By Joan Goodchild, Senior Editor

October 28, 2009 — CSO —

The words "swine flu" had barely been uttered last spring when spammers and malware authors, hoping to take advantage of fears and curiosity about the virus, began devising ways to trick people with clever subject lines and fake web sites. In April, only days after officials began to talk about the virus, officially known as H1N1, researchers with several security firms reported spam relating to the virus already accounted for 4 percent of all unwanted emails.

More than six months later, H1N1 has indeed spread to large numbers of people around the world. So have related scams and schemes cooked up by the bad guys, either looking to infect your computer, steal your credit card information or sell you phony products. Here, we detail some of the most common lines being used online lately.

For expert advice on business continuity in the face of the pandemic, check out CSO's Swine Flu (H1N1) Business Continuity Planning Guide

Treat swine flu virus! Buy Tamiflu without a prescription
Researchers at McAfee Labs have found that a great deal of the spam ending up in inboxes lately has a subject line that offers Tamiflu, a prescription-only medication that can stop influenza from further mutating in the early stages of the virus, without a prescription. According to McAfee Labs lead researcher Adam Wosotowsky, the link offering Tamiflu usually directs users back to an alleged Canadian pharmaceutical site that likely sells fake products. In fact, spam that advertises websites for "Canadian pharmaceuticals" accounted for more than 70 percent of global spam volume in September, according to McAfee analysis.

In the past few weeks, fraudulent offers of so-called swine flu treatments and medications have become so

ESSENTIAL READING

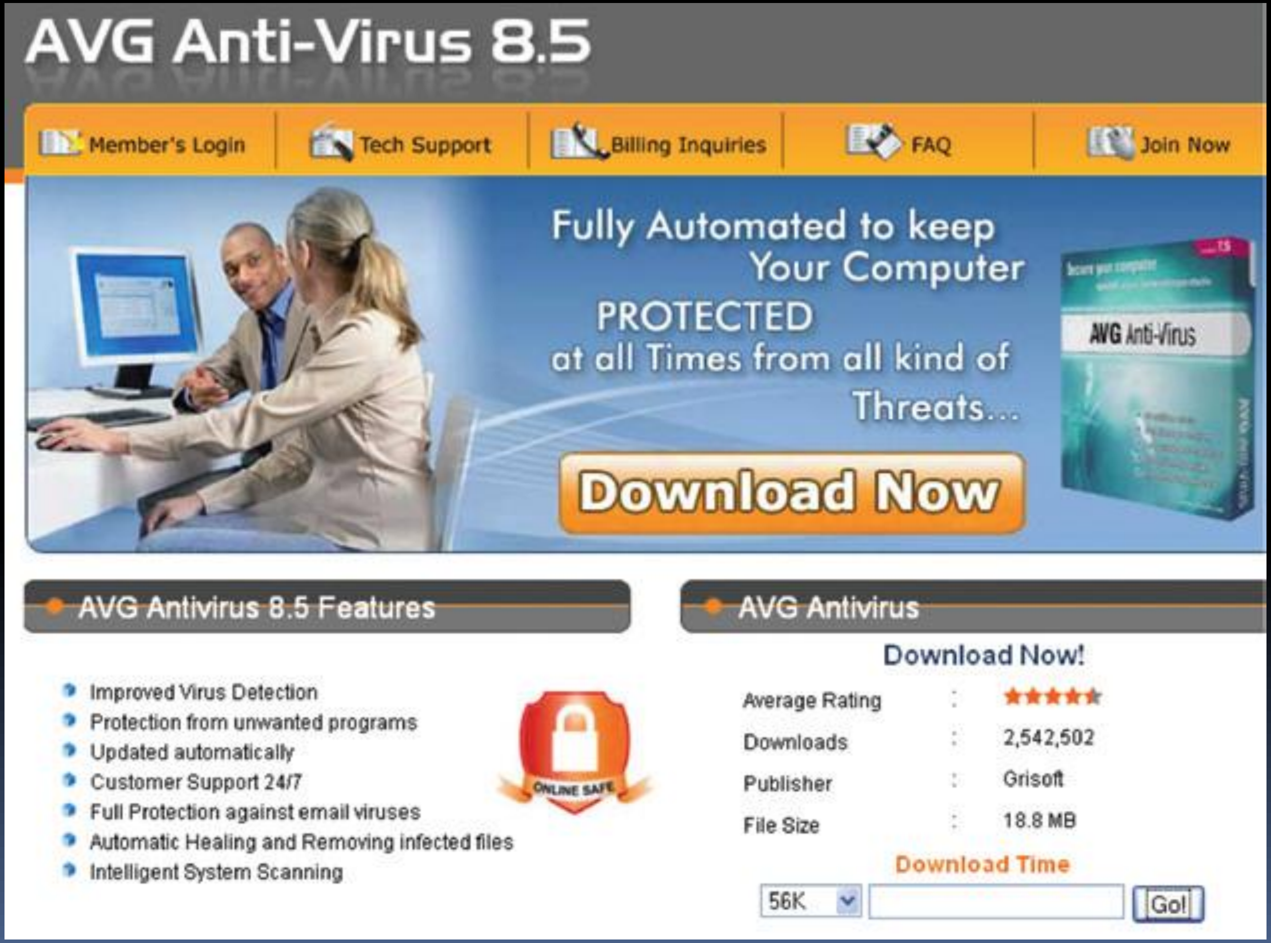
- Wireless Security Basics
- Network Security Basics
- Computer Incident Detection, Response, and Forensics
- A Few Good Information Security Metrics
- Breach Disclosure Laws by State (Map)

WEBCASTS

Mining for Gold: Cybercrime Prevention and the Role of Log Management

Done, but with errors on page.

Free solution? DO NOT CLICK ON THIS!!!



AVG Anti-Virus 8.5

Fully Automated to keep Your Computer PROTECTED at all Times from all kind of Threats...

AVG Antivirus 8.5 Features

- Improved Virus Detection
- Protection from unwanted programs
- Updated automatically
- Customer Support 24/7
- Full Protection against email viruses
- Automatic Healing and Removing infected files
- Intelligent System Scanning

AVG Antivirus

Download Now!

Average Rating : ★★★★★
Downloads : 2,542,502
Publisher : Grisoft
File Size : 18.8 MB

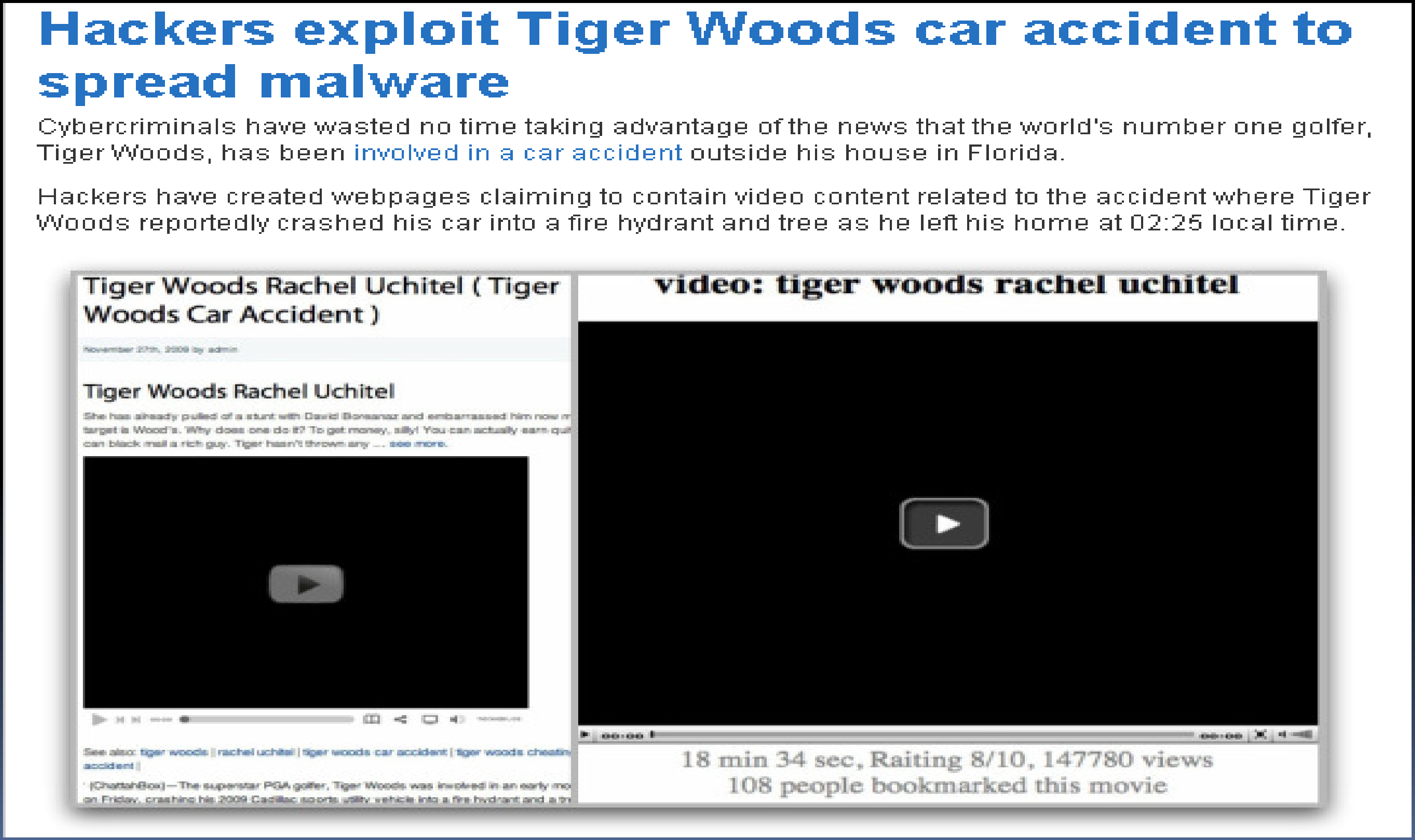
Download Time

56K

How about a new picture?

- One emerging attack on social networks, for example, sends messages to a victim's friends that he has updated his profile photo
- When the friends click on a link to the photo, they are then infected, as well, and the cycle continues

Or just plain take advantage of our desire for titillation



Hackers exploit Tiger Woods car accident to spread malware

Cybercriminals have wasted no time taking advantage of the news that the world's number one golfer, Tiger Woods, has been involved in a car accident outside his house in Florida.

Hackers have created webpages claiming to contain video content related to the accident where Tiger Woods reportedly crashed his car into a fire hydrant and tree as he left his home at 02:25 local time.

Tiger Woods Rachel Uchitel (Tiger Woods Car Accident)

November 27th, 2009 by admin

Tiger Woods Rachel Uchitel

She has already pulled of a stunt with David Boreanaz and embarrassed him now m
target is Wood's. Why does one do it? To get money, silly! You can actually earn qui
can black mail a rich guy. Tiger hasn't thrown any .... see more.

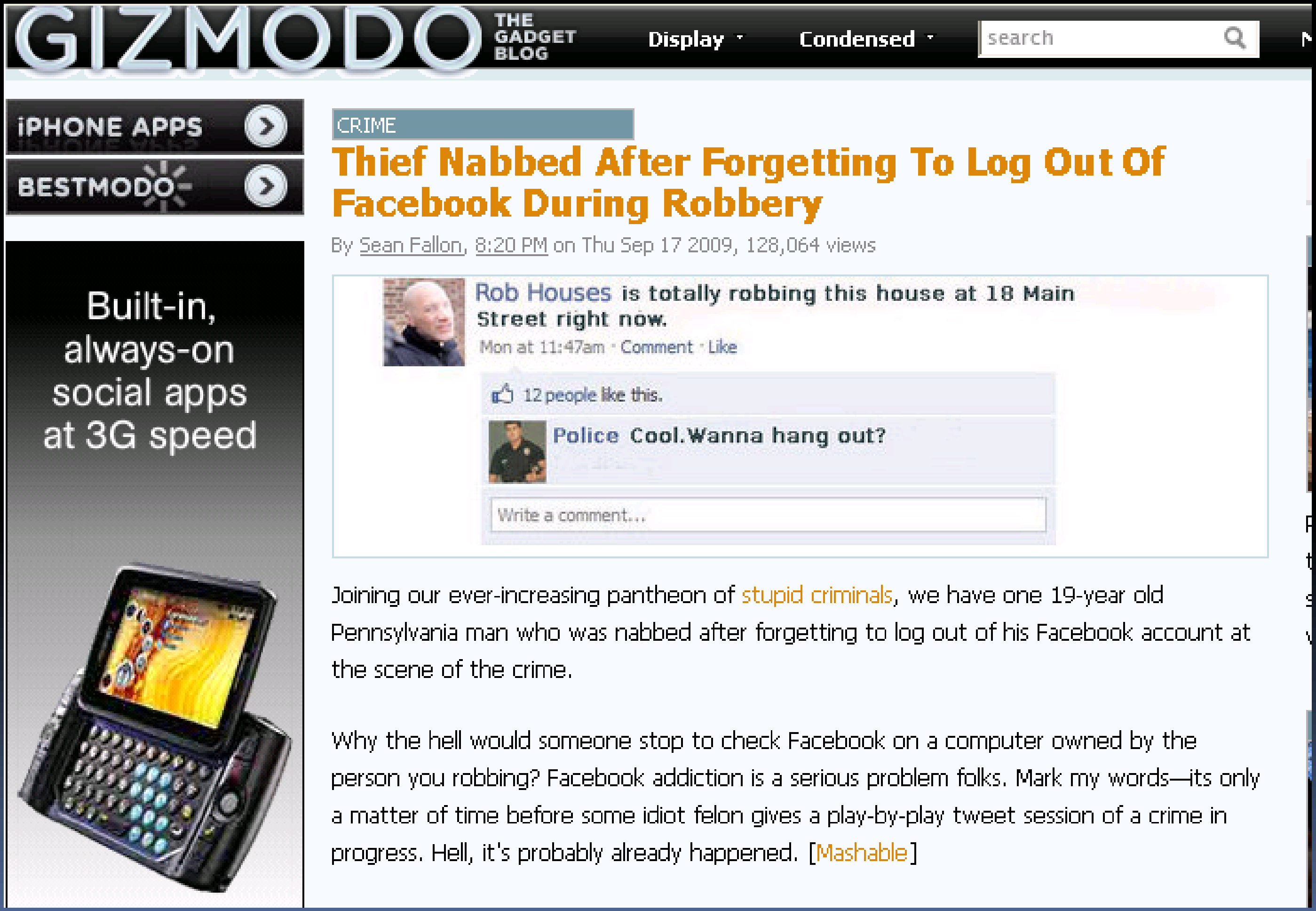
See also: tiger woods | rachel uchitel | tiger woods car accident | tiger woods cheatin
accident |

' (ChattahBox)—The superstar PGA golfer, Tiger Woods was involved in an early mo
on Friday, crashing his 2009 Cadillac sports utility vehicle into a fire hydrant and a tr

video: tiger woods rachel uchitel

18 min 34 sec, Raiting 8/10, 147780 views
108 people bookmarked this movie

Life is tough but it's tougher when you're stupid!



CRIME

Thief Nabbed After Forgetting To Log Out Of Facebook During Robbery

By Sean Fallon, 8:20 PM on Thu Sep 17 2009, 128,064 views

Rob Houses is totally robbing this house at 18 Main Street right now.
Mon at 11:47am · Comment · Like

12 people like this.

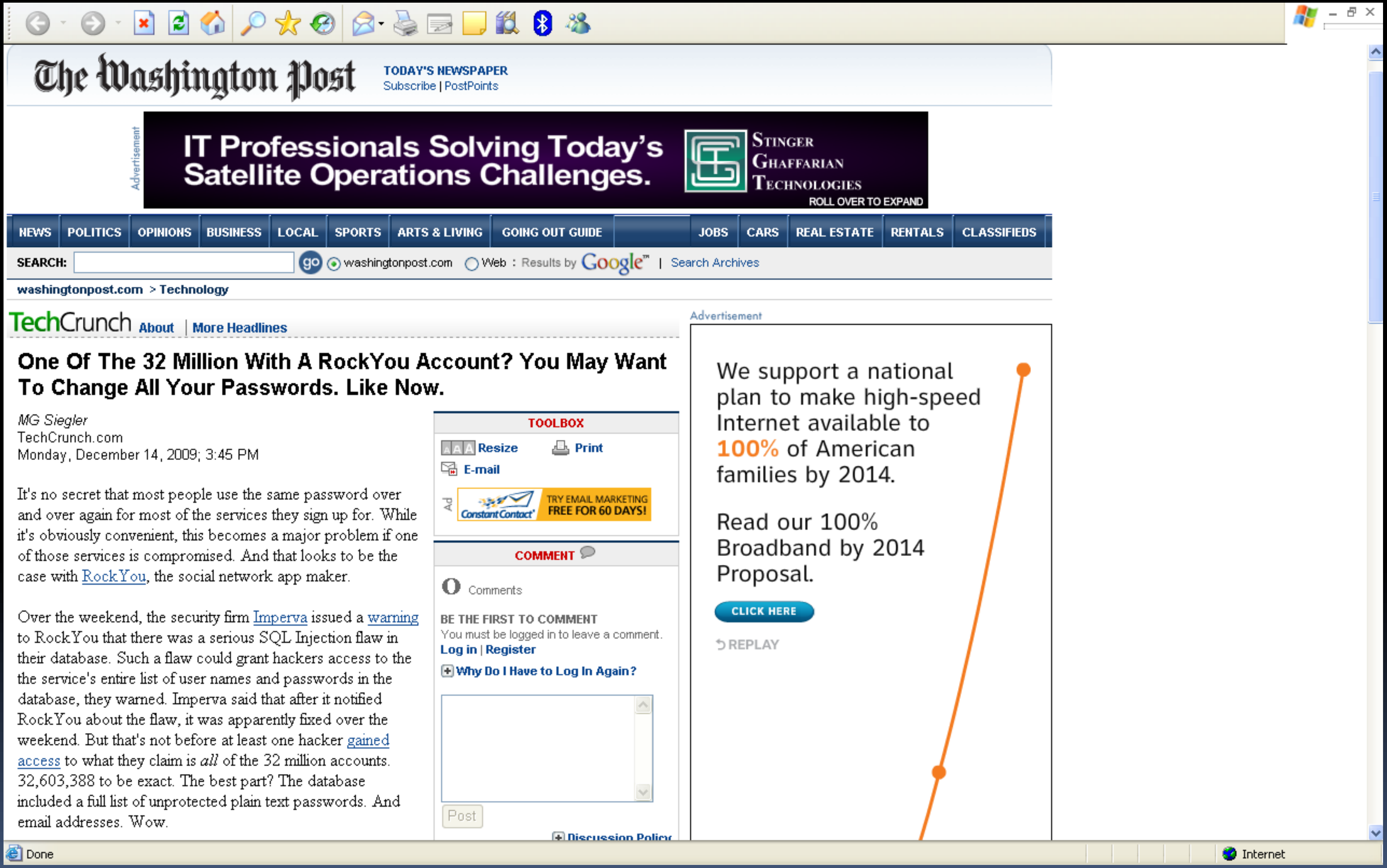
Police Cool.Wanna hang out?

Write a comment...

Joining our ever-increasing pantheon of stupid criminals, we have one 19-year old Pennsylvania man who was nabbed after forgetting to log out of his Facebook account at the scene of the crime.

Why the hell would someone stop to check Facebook on a computer owned by the person you robbing? Facebook addiction is a serious problem folks. Mark my words—its only a matter of time before some idiot felon gives a play-by-play tweet session of a crime in progress. Hell, it's probably already happened. [Mashable]

Yesterday



One Of The 32 Million With A RockYou Account? You May Want To Change All Your Passwords. Like Now.

MG Siegler
TechCrunch.com
Monday, December 14, 2009; 3:45 PM

It's no secret that most people use the same password over and over again for most of the services they sign up for. While it's obviously convenient, this becomes a major problem if one of those services is compromised. And that looks to be the case with RockYou, the social network app maker.

Over the weekend, the security firm Imperva issued a warning to RockYou that there was a serious SQL Injection flaw in their database. Such a flaw could grant hackers access to the the service's entire list of user names and passwords in the database, they warned. Imperva said that after it notified RockYou about the flaw, it was apparently fixed over the weekend. But that's not before at least one hacker gained access to what they claim is *all* of the 32 million accounts. 32,603,388 to be exact. The best part? The database included a full list of unprotected plain text passwords. And email addresses. Wow.

We support a national plan to make high-speed Internet available to 100% of American families by 2014.

Read our 100% Broadband by 2014 Proposal.

Same old, same old

- It's no secret that most people use the same password over and over again for most of the services they sign up for
- While it's obviously convenient, this becomes a major problem if one of those services is compromised.
- And that looks to be the case with RockYou, the social network app maker

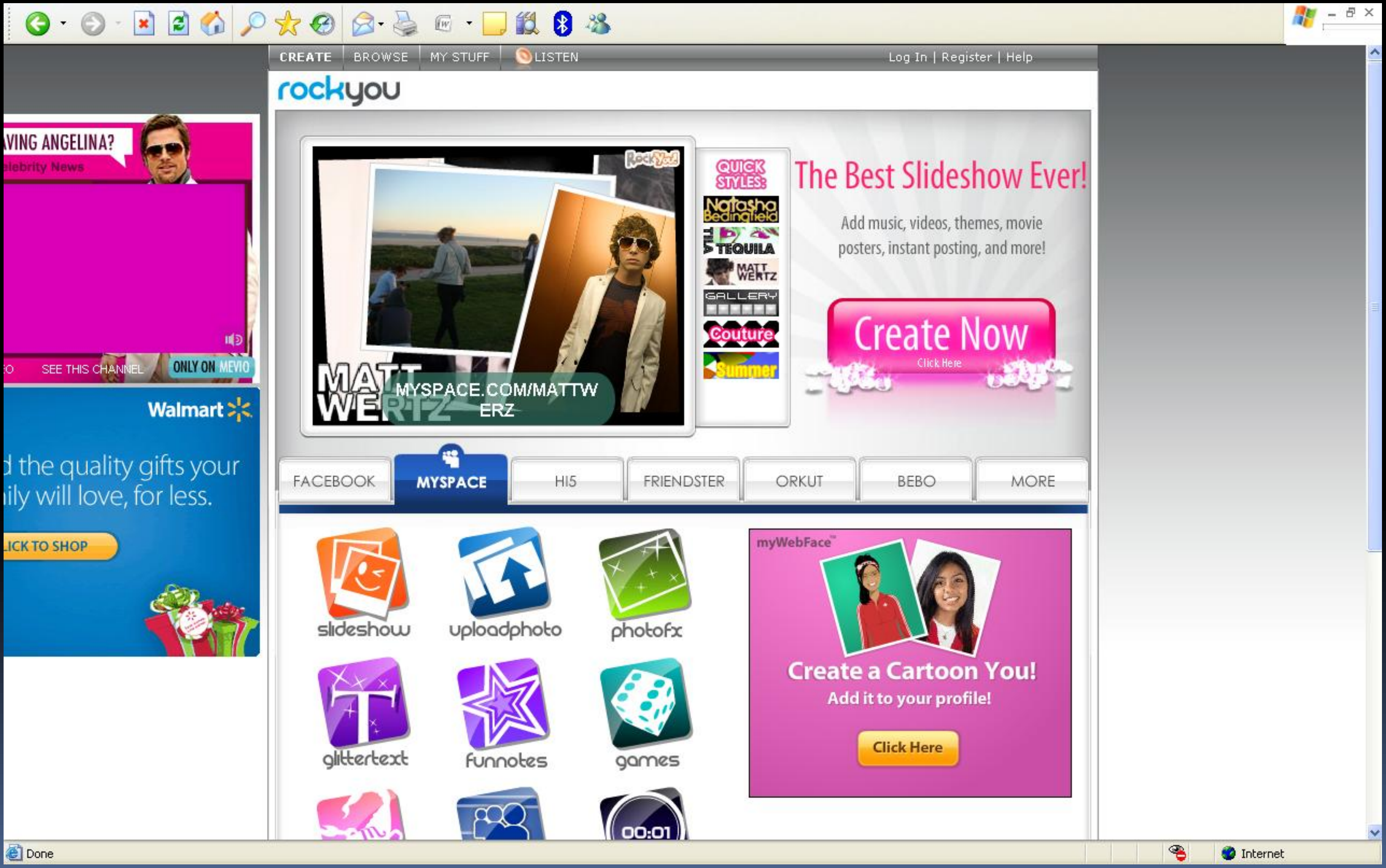
The sounds of silence

- To compound the severity of the security breach, it was found that RockYou are storing all user account data in plain text in their database, exposing all that information to attackers
- RockYou have yet to inform users of the breach, and their blog is eerily silent – but the details of the security breach are going from bad to worse

Head in the sand

- The hacker responsible for the initial breach published a small portion of the dataset he had retrieved and was able to show that not only did he have access to their entire database, but also passwords were stored in the clear

Totally compromised



This begs the question…

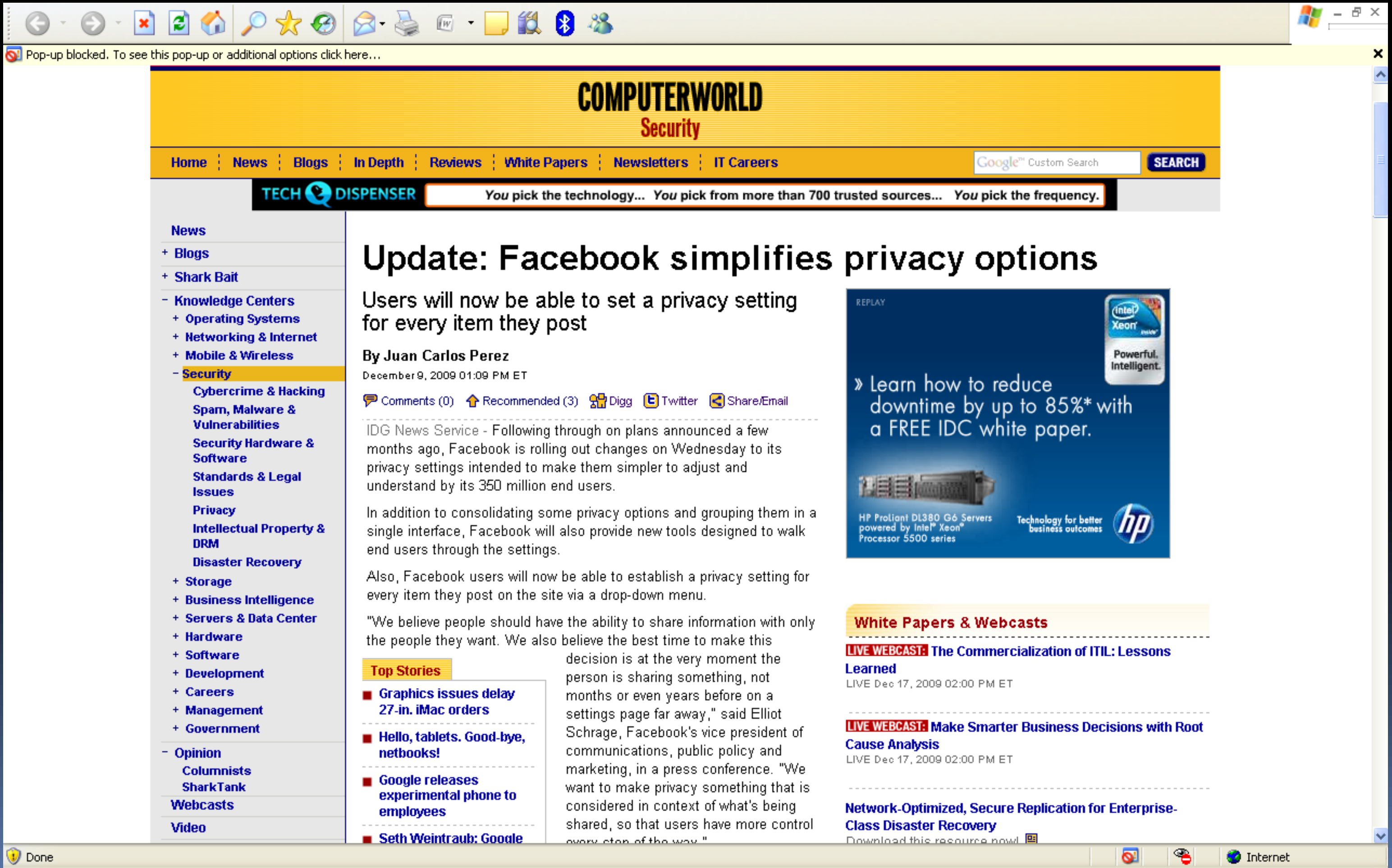
- How many people use the same password for each and every social site?
- I would venture that a vast majority of the 32,000,000 users whose data was compromised

© Corbis

Okay to trust but please verify

A healthy dose of skepticism

Please take the time to change your privacy options but only do so at facebook.com and not at some duck's site!



Pop-up blocked. To see this pop-up or additional options click here...

COMPUTERWORLD
Security

Home | News | Blogs | In Depth | Reviews | White Papers | Newsletters | IT Careers

Google™ Custom Search SEARCH

- News
- + Blogs
- + Shark Bait
- − Knowledge Centers
  - + Operating Systems
  - + Networking & Internet
  - + Mobile & Wireless
  - − Security
    - Cybercrime & Hacking
    - Spam, Malware & Vulnerabilities
    - Security Hardware & Software
    - Standards & Legal Issues
    - Privacy
    - Intellectual Property & DRM
    - Disaster Recovery
  - + Storage
  - + Business Intelligence
  - + Servers & Data Center
  - + Hardware
  - + Software
  - + Development
  - + Careers
  - + Management
  - + Government
- − Opinion
  - Columnists
  - SharkTank
- Webcasts
- Video

Update: Facebook simplifies privacy options

Users will now be able to set a privacy setting for every item they post

By Juan Carlos Perez

December 9, 2009 01:09 PM ET

Comments (0) Recommended (3) Digg Twitter Share/Email

IDG News Service - Following through on plans announced a few months ago, Facebook is rolling out changes on Wednesday to its privacy settings intended to make them simpler to adjust and understand by its 350 million end users.

In addition to consolidating some privacy options and grouping them in a single interface, Facebook will also provide new tools designed to walk end users through the settings.

Also, Facebook users will now be able to establish a privacy setting for every item they post on the site via a drop-down menu.

"We believe people should have the ability to share information with only the people they want. We also believe the best time to make this decision is at the very moment the person is sharing something, not months or even years before on a settings page far away," said Elliot Schrage, Facebook's vice president of communications, public policy and marketing, in a press conference. "We want to make privacy something that is considered in context of what's being shared, so that users have more control every step of the way."

Top Stories

- Graphics issues delay 27-in. iMac orders
- Hello, tablets. Good-bye, netbooks!
- Google releases experimental phone to employees
- Seth Weintraub: Google

White Papers & Webcasts

LIVE WEBCAST: The Commercialization of ITIL: Lessons Learned
LIVE Dec 17, 2009 02:00 PM ET

LIVE WEBCAST: Make Smarter Business Decisions with Root Cause Analysis
LIVE Dec 17, 2009 02:00 PM ET

Network-Optimized, Secure Replication for Enterprise-Class Disaster Recovery
Download this resource now!

Done   Internet

Lock it down!

So, what's the solution, Patrick?

- The decision to embrace social media technology is a risk-based decision, not a technology-based decision
- It must be made based on a strong business case, supported at the appropriate level for each department or agency, considering its mission space, threats, technical capabilities, and potential benefits

Just say yes, but secure it

- The goal of the IT organization should not be to say “No” to social media websites and block them completely, but to say “Yes, following security guidance,” with effective and appropriate information assurance security and privacy controls

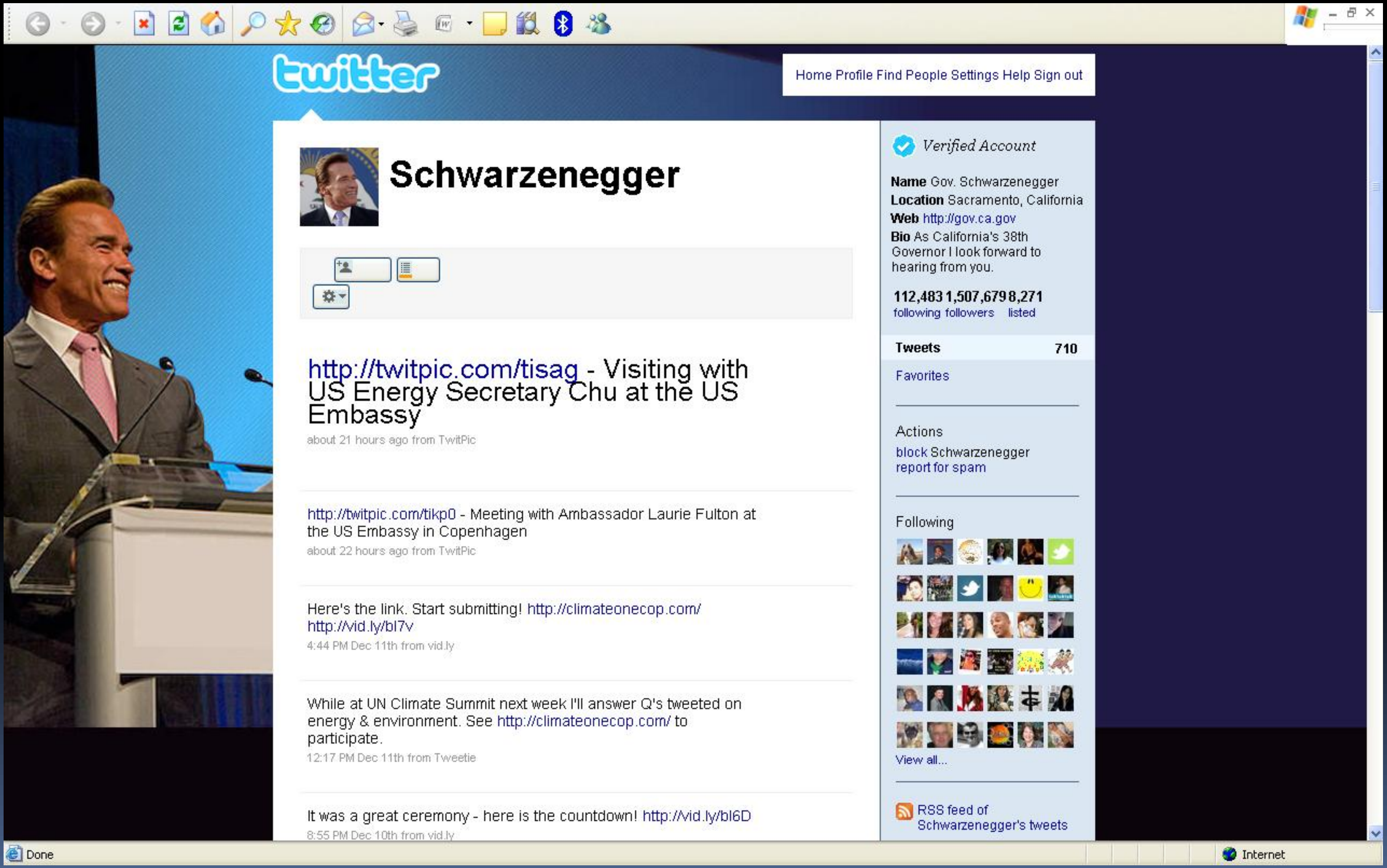
A well thought out decision

- The decision to authorize access to social media websites is a business decision, and comes from a risk management process made by the management team with inputs from all players, including the CIO, CISO, Office of General Counsel (OGC), privacy official and the mission owner

Aggressive threats

- The use of social media and the inherent cybersecurity concerns form a complex topic that introduces additional vulnerabilities, targeted by an advanced threat, requiring updated sets of controls
- Your information systems are targeted by persistent, pervasive, aggressive threats – and should not be glossed over

Hey, who's going to tell him he can't?



Schwarzenegger

http://twitpic.com/tisag - Visiting with US Energy Secretary Chu at the US Embassy
about 21 hours ago from TwitPic

http://twitpic.com/tikp0 - Meeting with Ambassador Laurie Fulton at the US Embassy in Copenhagen
about 22 hours ago from TwitPic

Here's the link. Start submitting! http://climateonecop.com/ http://vid.ly/bl7v
4:44 PM Dec 11th from vid.ly

While at UN Climate Summit next week I'll answer Q's tweeted on energy & environment. See http://climateonecop.com/ to participate.
12:17 PM Dec 11th from Tweetie

It was a great ceremony - here is the countdown! http://vid.ly/bl6D
8:55 PM Dec 10th from vid.ly

Verified Account

Name Gov. Schwarzenegger
Location Sacramento, California
Web http://gov.ca.gov
Bio As California's 38th Governor I look forward to hearing from you.

112,483	1,507,679	8,271
following	followers	listed

Tweets 710

Favorites

Actions
block Schwarzenegger
report for spam

Following

View all...

RSS feed of Schwarzenegger's tweets

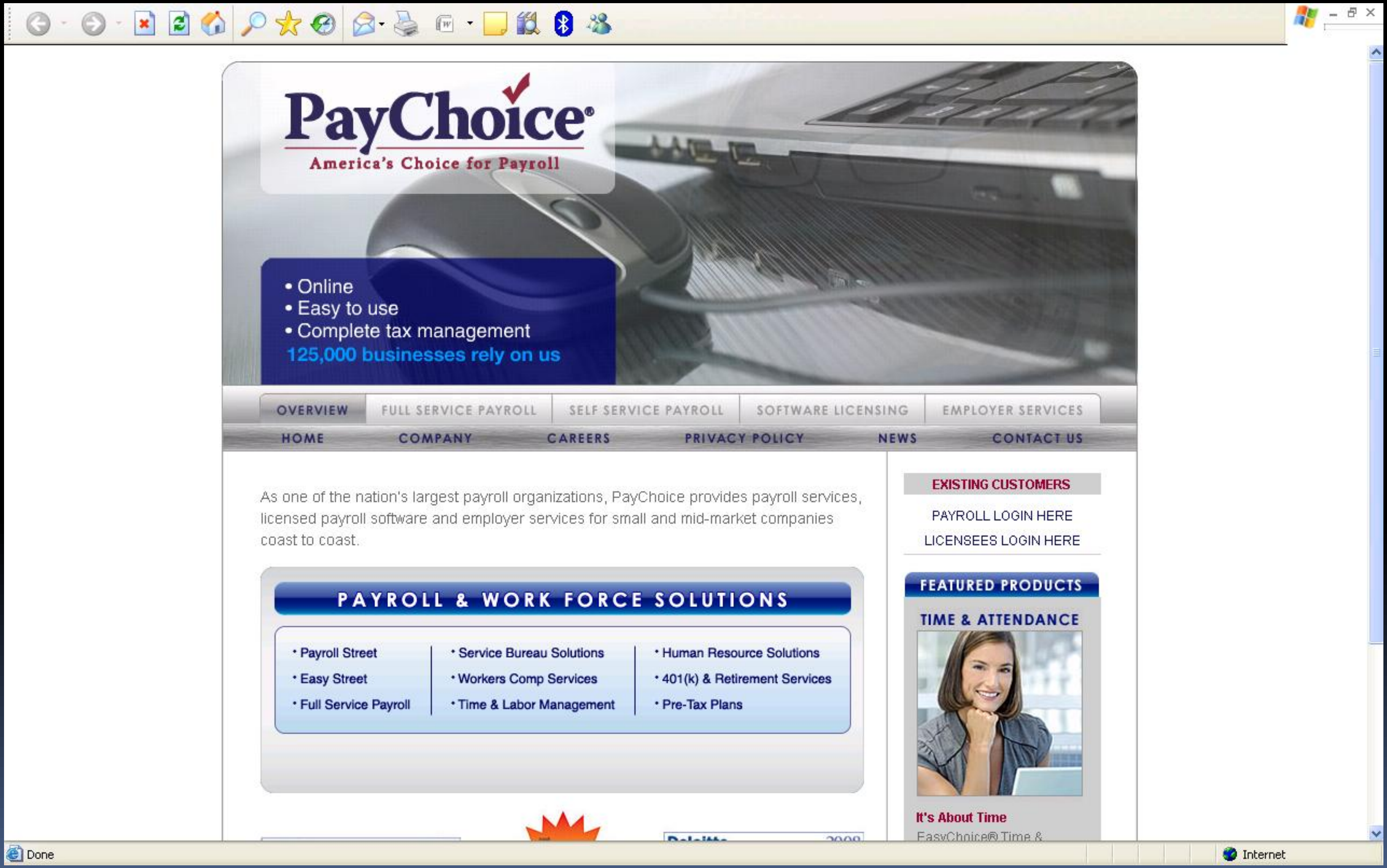
So, have fun!

digg
YouTube
Broadcast Yourself
upcoming.org
last.fm
the social music revolution
flickr
BETA
myspace.com
Technorati
twitter
facebook.
MyBlogLog
slideshare
jaiku

Email – an enticing vector

Aunt Marion

PayChoice



- Online
- Easy to use
- Complete tax management

125,000 businesses rely on us

As one of the nation's largest payroll organizations, PayChoice provides payroll services, licensed payroll software and employer services for small and mid-market companies coast to coast.

PAYROLL & WORK FORCE SOLUTIONS

- Payroll Street
- Easy Street
- Full Service Payroll
- Service Bureau Solutions
- Workers Comp Services
- Time & Labor Management
- Human Resource Solutions
- 401(k) & Retirement Services
- Pre-Tax Plans

It's About Time

EasyChoice® Time &

Misdirection

- Last Wednesday, a number of PayChoice customers received an e-mail warning them that they needed to download a Web browser plug-in in order to maintain uninterrupted access to the portal for PayChoice's online payroll service
- The supposed plug-in was instead malicious software designed to steal the victim's user names and passwords
- Remember, they want to take you someplace else

So,

- If we understand these burgeoning threats and deploy appropriate security solutions, we can stay a step ahead of the black hats as they target the social networking sites

Gartner Group Quote on Security

- ***"Executives must get employees on board and establish a corporate culture that endorses security. Culture is probably the single biggest influence in an enterprise. We need to start thinking about security as a business enabler."***

Richard Mogull, Former Security Analyst
Gartner Group

But what does that mean?

- I am just a State employee and am not an engineer or a technician or a programmer or a geek!
- I'm just sitting at my desk, talking to citizens or other State employees
- How in the world am I threatening the State's network???

2 Reasons…

- You probably do not understand policies, procedures, best practices and standards
- If you do understand them, they are violated because there are no consequences – the policies are not enforced
- Who, me?

There is a human element to all of this, an element that is more often than not, overlooked…

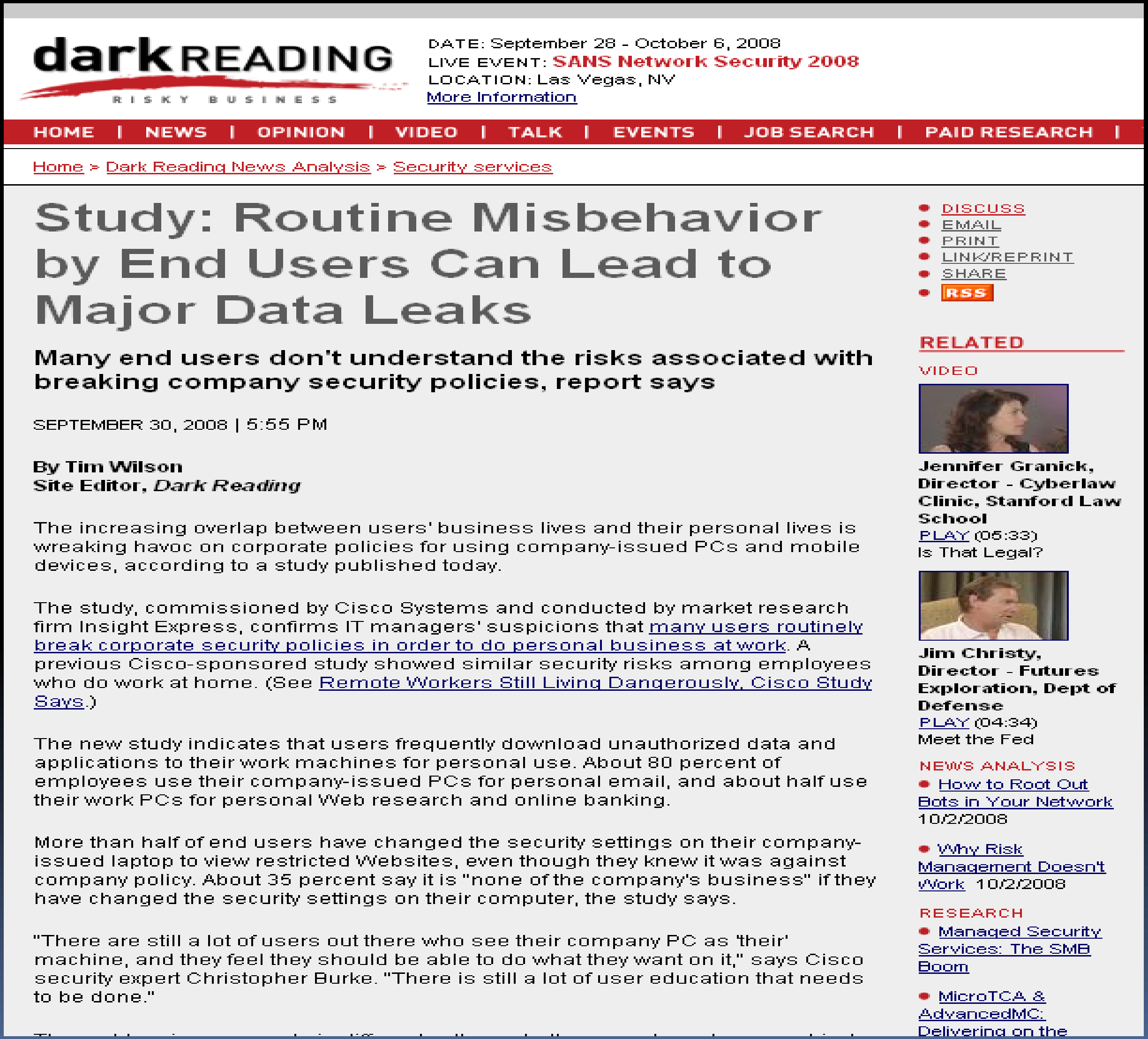
You Must Understand…

- That California is a target
- These hackers are smart, and most have much more time to spend attacking them than a typical system administrator can spend defending against them

Education is Critical

- Few executives grasp the case for investing in safeguards against hackers, worms, and the like
- Education starts at the top and works its way down the food chain throughout the entire State
- Before any California State employee puts their fingers on the keyboard they must understand that it is not ***their*** computer

Survey says…



darkREADING
RISKY BUSINESS

HOME | NEWS | OPINION | VIDEO | TALK | EVENTS | JOB SEARCH | PAID RESEARCH |
Home > Dark Reading News Analysis > Security services

Study: Routine Misbehavior by End Users Can Lead to Major Data Leaks

Many end users don't understand the risks associated with breaking company security policies, report says

SEPTEMBER 30, 2008 | 5:55 PM

By Tim Wilson
Site Editor, *Dark Reading*

The increasing overlap between users' business lives and their personal lives is wreaking havoc on corporate policies for using company-issued PCs and mobile devices, according to a study published today.

The study, commissioned by Cisco Systems and conducted by market research firm Insight Express, confirms IT managers' suspicions that many users routinely break corporate security policies in order to do personal business at work. A previous Cisco-sponsored study showed similar security risks among employees who do work at home. (See Remote Workers Still Living Dangerously, Cisco Study Says.)

The new study indicates that users frequently download unauthorized data and applications to their work machines for personal use. About 80 percent of employees use their company-issued PCs for personal email, and about half use their work PCs for personal Web research and online banking.

More than half of end users have changed the security settings on their company-issued laptop to view restricted Websites, even though they knew it was against company policy. About 35 percent say it is "none of the company's business" if they have changed the security settings on their computer, the study says.

"There are still a lot of users out there who see their company PC as 'their' machine, and they feel they should be able to do what they want on it," says Cisco security expert Christopher Burke. "There is still a lot of user education that needs to be done."

RELATED

VIDEO

Jennifer Granick, Director - Cyberlaw Clinic, Stanford Law School
PLAY (05:33)
Is That Legal?

Jim Christy, Director - Futures Exploration, Dept of Defense
PLAY (04:34)
Meet the Fed

NEWS ANALYSIS

- How to Root Out Bots in Your Network 10/2/2008
- Why Risk Management Doesn't Work 10/2/2008

RESEARCH

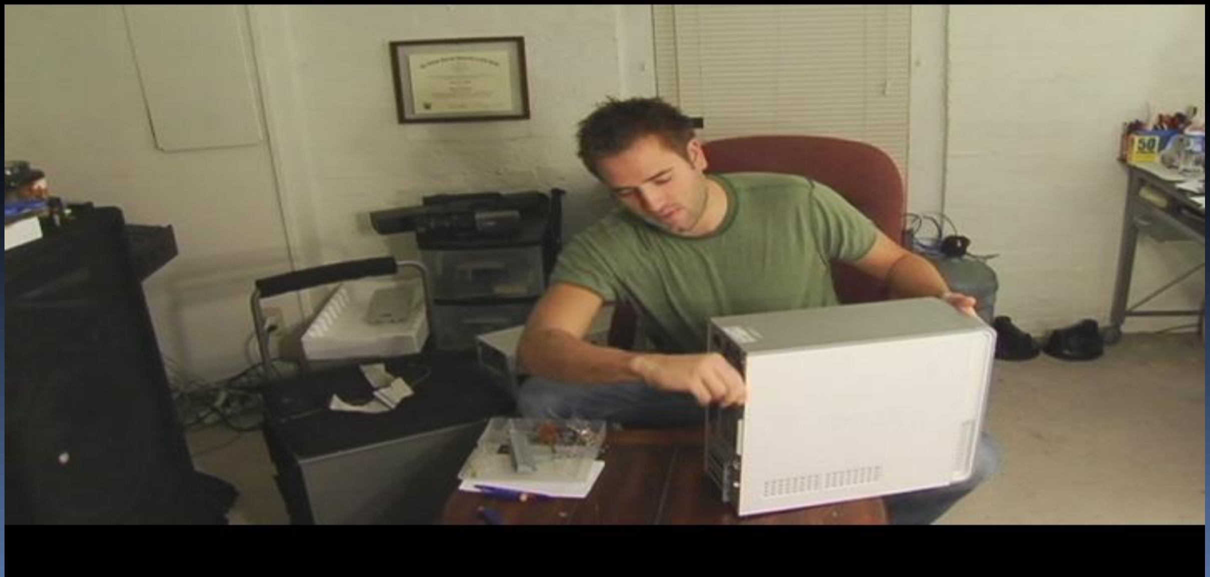
- Managed Security Services: The SMB Boom
- MicroTCA & AdvancedMC: Delivering on the

Findings

- Users frequently download unauthorized data and applications to their work machines for personal use
- About 80 percent of employees use their State-issued PCs for personal email, and about half use their work PCs for personal Web research and online banking

Routine Behavior

- More than half of end users have changed the security settings on their State-issued computer to view restricted Websites, even though they knew it was against policy



Findings

- About 35 percent say it is "none of their employer's business" if they have changed the security settings on their computer
- There are still a lot of users out there who see their issued PC as 'their' machine, and they feel they should be able to do what they want on it

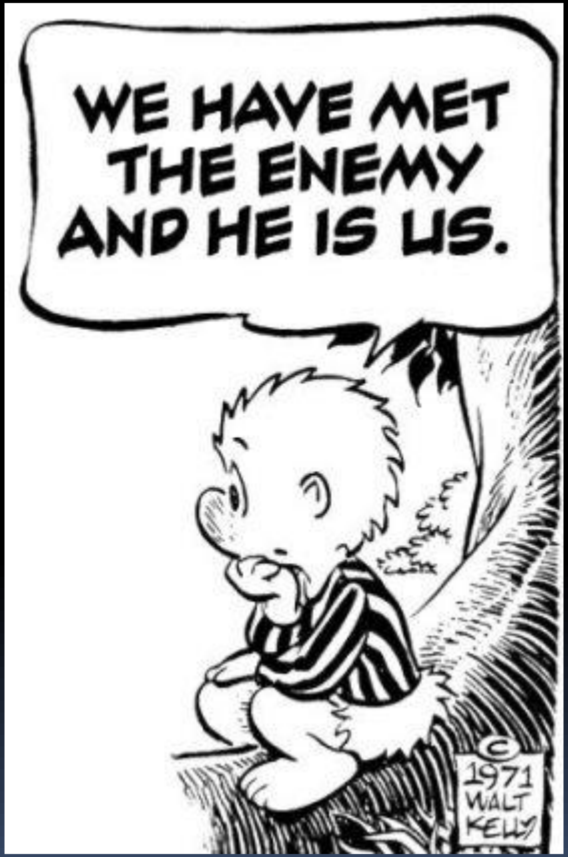
Findings

- More than half of IT execs say that such unauthorized activity causes as much as 25 percent of the data leakage in their organizations; 16 percent say it causes up to 50 percent
- Many users also share both company devices and sensitive information with others, including colleagues, friends, and family members

Findings

- More than 40 percent of the users said they shared sensitive information because they felt the need to "bounce an idea off of someone."
- About 30 percent said they felt the need to vent and/or didn't see anything wrong with sharing the sensitive information

Pogo was right…



The State of Security Today: active vs. passive

Passive…

What good is security if no one is

And try to understand the *real* threat!

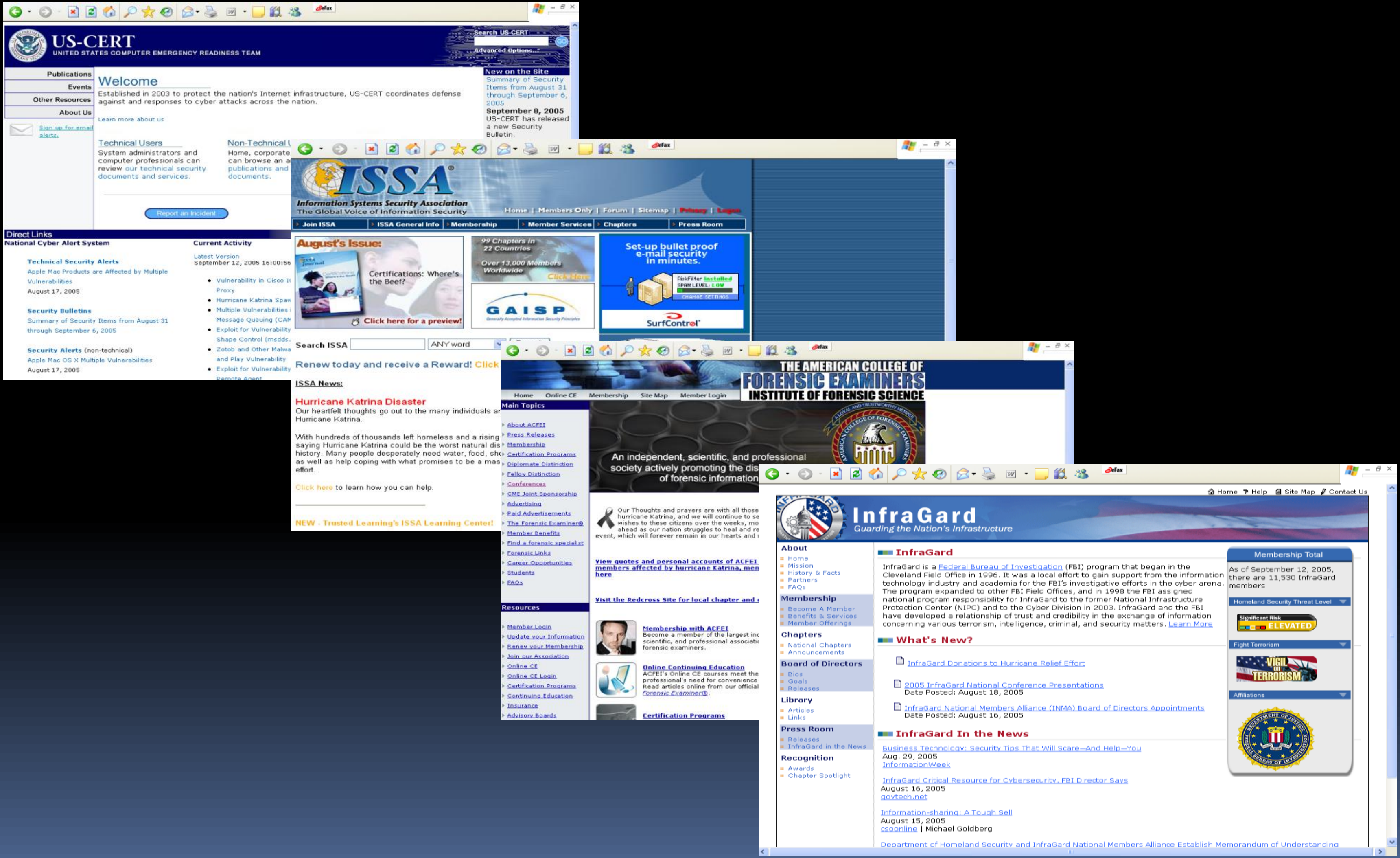
Get an
Information Security Risk Assessment!

The Seven Deadly Sins of Network Security

1. Not measuring risk
2. Thinking compliance equals security
3. Overlooking the people
4. Too much access for too many
5. Lax patching procedures
6. Lax logging, monitoring
7. Spurning the K.I.S.S.

The Insider is hard to Identify

Collaborate



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Search US-CERT
Advanced Options...

Publications
Events
Other Resources
About Us

Sign up for email alerts.

Welcome

Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

Learn more about us

New on the Site
Summary of Security Items from August 31 through September 6, 2005
September 8, 2005
US-CERT has released a new Security Bulletin.

Technical Users
System administrators and computer professionals can review our technical security documents and services.

Non-Technical U
Home, corporate
can browse an a
publications and
documents.

Report an Incident

Direct Links

National Cyber Alert System

Technical Security Alerts
Apple Mac Products are Affected by Multiple Vulnerabilities
August 17, 2005

Security Bulletins
Summary of Security Items from August 31 through September 6, 2005

Security Alerts (non-technical)
Apple Mac OS X Multiple Vulnerabilities
August 17, 2005

Current Activity
Latest Version
September 12, 2005 16:00:56

- Vulnerability in Cisco IC Proxy
- Hurricane Katrina Spaw
- Multiple Vulnerabilities i Message Queuing (CAM
- Exploit for Vulnerability Shape Control (msdds.
- Zotob and Other Malwa and Play Vulnerability
- Exploit for Vulnerability Remote Agent

ISSA®
Information Systems Security Association
The Global Voice of Information Security

Home | Members Only | Forum | Sitemap | Privacy | Logout

Join ISSA | ISSA General Info | Membership | Member Services | Chapters | Press Room

August's Issue:
Certifications: Where's the Beef?
Click here for a preview!

99 Chapters in 22 Countries
Over 13,000 Members Worldwide
Click Here

GAISP
Generally Accepted Information Security Principles

Set-up bullet proof e-mail security in minutes.
RiskFilter Installed
SPAM LEVEL: LOW
CHANGE SETTINGS
SurfControl®

Search ISSA ANY word

Renew today and receive a Reward! Click

ISSA News:

Hurricane Katrina Disaster
Our heartfelt thoughts go out to the many individuals ar
Hurricane Katrina.

With hundreds of thousands left homeless and a rising
saying Hurricane Katrina could be the worst natural dis
history. Many people desperately need water, food, she
as well as help coping with what promises to be a mas
effort.

Click here to learn how you can help.

NEW - Trusted Learning's ISSA Learning Center!

THE AMERICAN COLLEGE OF FORENSIC EXAMINERS
INSTITUTE OF FORENSIC SCIENCE

Home | Online CE | Membership | Site Map | Member Login

Main Topics
- About ACFEI
- Press Releases
- Membership
- Certification Programs
- Diplomate Distinction
- Fellow Distinction
- Conferences
- CME Joint Sponsorship
- Advertising
- Paid Advertisements
- The Forensic Examiner®
- Member Benefits
- Find a forensic specialist
- Forensic Links
- Career Opportunities
- Students
- FAQs

Resources
- Member Login
- Update your Information
- Renew your Membership
- Join our Association
- Online CE
- Online CE Login
- Certification Programs
- Continuing Education
- Insurance
- Advisory Boards

An independent, scientific, and professional
society actively promoting the dis
of forensic information

Our Thoughts and prayers are with all those
hurricane Katrina, and we will continue to se
wishes to these citizens over the weeks, mo
ahead as our nation struggles to heal and re
event, which will forever remain in our hearts and i

View quotes and personal accounts of ACFEI
members affected by hurricane Katrina, men
here

Visit the Redcross Site for local chapter and

Membership with ACFEI
Become a member of the largest inc
scientific, and professional associati
forensic examiners.

Online Continuing Education
ACFEI's Online CE courses meet the
professional's need for convenience
Read articles online from our official
Forensic Examiner®.

Certification Programs

Home | Help | Site Map | Contact Us

InfraGard
Guarding the Nation's Infrastructure

About
- Home
- Mission
- History & Facts
- Partners
- FAQs

Membership
- Become A Member
- Benefits & Services
- Member Offerings

Chapters
- National Chapters
- Announcements

Board of Directors
- Bios
- Goals
- Releases

Library
- Articles
- Links

Press Room
- Releases
- InfraGard in the News

Recognition
- Awards
- Chapter Spotlight

InfraGard

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. Learn More

What's New?

InfraGard Donations to Hurricane Relief Effort

2005 InfraGard National Conference Presentations
Date Posted: August 18, 2005

InfraGard National Members Alliance (INMA) Board of Directors Appointments
Date Posted: August 16, 2005

InfraGard In the News

Business Technology: Security Tips That Will Scare--And Help--You
Aug. 29, 2005
InformationWeek

InfraGard Critical Resource for Cybersecurity, FBI Director Says
August 16, 2005
govtech.net

Information-sharing: A Tough Sell
August 15, 2005
csoonline | Michael Goldberg

Department of Homeland Security and InfraGard National Members Alliance Establish Memorandum of Understanding

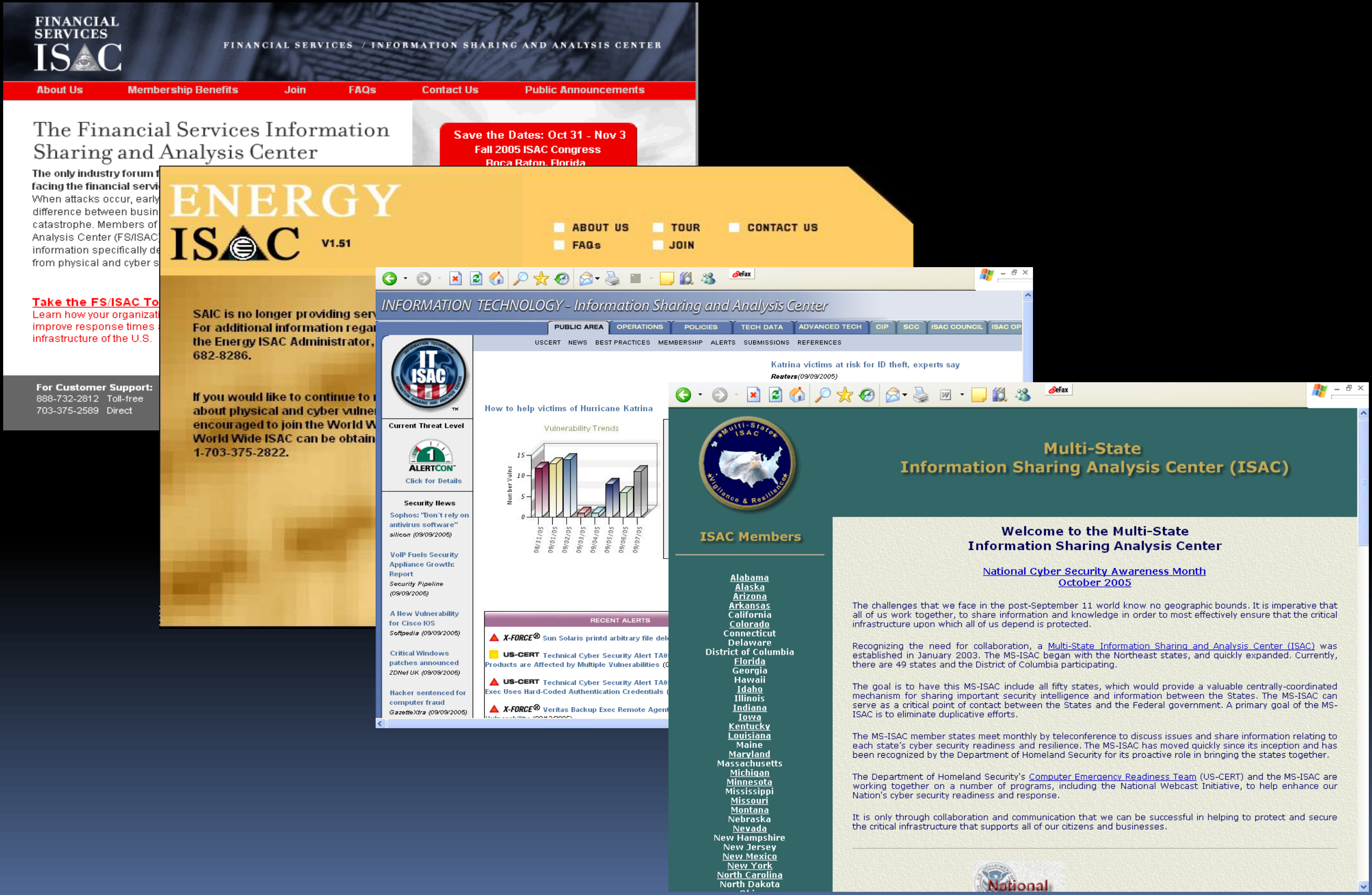
Membership Total
As of September 12, 2005, there are 11,530 InfraGard members

Homeland Security Threat Level
Significant Risk
ELEVATED

Fight Terrorism
VIGIL on TERRORISM

Affiliations

Do we share?



FINANCIAL SERVICES ISAC

FINANCIAL SERVICES / INFORMATION SHARING AND ANALYSIS CENTER

The Financial Services Information Sharing and Analysis Center

The only industry forum f
facing the financial servi
When attacks occur, early
difference between busin
catastrophe. Members of
Analysis Center (FS/ISAC)
information specifically de
from physical and cyber s

Save the Dates: Oct 31 - Nov 3
Fall 2005 ISAC Congress
Boca Raton, Florida

Take the FS/ISAC To
Learn how your organizat
improve response times
infrastructure of the U.S.

For Customer Support:
888-732-2812 Toll-free
703-375-2589 Direct

ENERGY ISAC V1.51

SAIC is no longer providing ser
For additional information rega
the Energy ISAC Administrator,
682-8286.

If you would like to continue to r
about physical and cyber vulner
encouraged to join the World W
World Wide ISAC can be obtain
1-703-375-2822.

INFORMATION TECHNOLOGY - Information Sharing and Analysis Center

Katrina victims at risk for ID theft, experts say
Reuters(09/09/2005)

How to help victims of Hurricane Katrina

Security News

Sophos: "Don't rely on antivirus software"
silicon (09/09/2005)

VoIP Fuels Security Appliance Growth: Report
Security Pipeline (09/09/2005)

A New Vulnerability for Cisco IOS
Softpedia (09/09/2005)

Critical Windows patches announced
ZDNet UK (09/09/2005)

Hacker sentenced for computer fraud
GazetteXtra (09/09/2005)

RECENT ALERTS

X-FORCE® Sun Solaris printd arbitrary file del
US-CERT Technical Cyber Security Alert TA0
Products are Affected by Multiple Vulnerabilities (
US-CERT Technical Cyber Security Alert TA0
Exec Uses Hard-Coded Authentication Credentials (
X-FORCE® Veritas Backup Exec Remote Agent

Multi-State Information Sharing Analysis Center (ISAC)

ISAC Members

Alabama
Alaska
Arizona
Arkansas
California
Colorado
Connecticut
Delaware
District of Columbia
Florida
Georgia
Hawaii
Idaho
Illinois
Indiana
Iowa
Kentucky
Louisiana
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
Montana
Nebraska
Nevada
New Hampshire
New Jersey
New Mexico
New York
North Carolina
North Dakota

Welcome to the Multi-State
Information Sharing Analysis Center

National Cyber Security Awareness Month
October 2005

The challenges that we face in the post-September 11 world know no geographic bounds. It is imperative that all of us work together, to share information and knowledge in order to most effectively ensure that the critical infrastructure upon which all of us depend is protected.

Recognizing the need for collaboration, a Multi-State Information Sharing and Analysis Center (ISAC) was established in January 2003. The MS-ISAC began with the Northeast states, and quickly expanded. Currently, there are 49 states and the District of Columbia participating.

The goal is to have this MS-ISAC include all fifty states, which would provide a valuable centrally-coordinated mechanism for sharing important security intelligence and information between the States. The MS-ISAC can serve as a critical point of contact between the States and the Federal government. A primary goal of the MS-ISAC is to eliminate duplicative efforts.

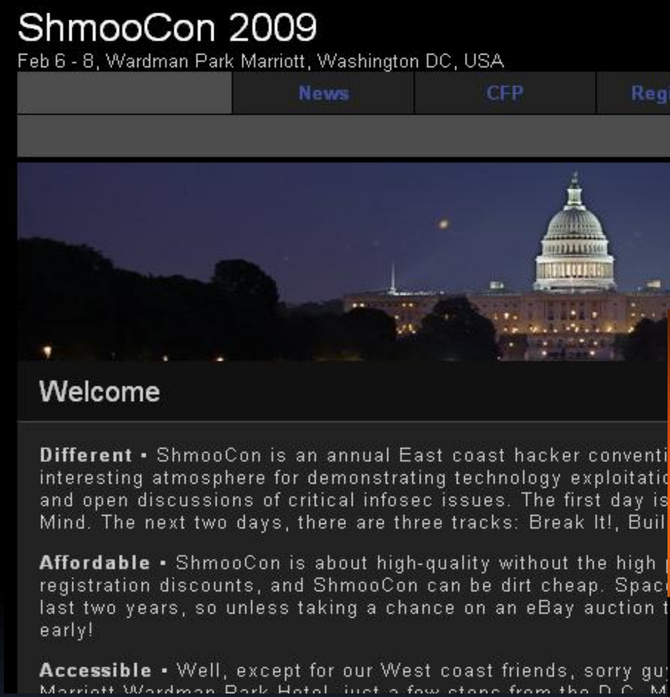
The MS-ISAC member states meet monthly by teleconference to discuss issues and share information relating to each state's cyber security readiness and resilience. The MS-ISAC has moved quickly since its inception and has been recognized by the Department of Homeland Security for its proactive role in bringing the states together.

The Department of Homeland Security's Computer Emergency Readiness Team (US-CERT) and the MS-ISAC are working together on a number of programs, including the National Webcast Initiative, to help enhance our Nation's cyber security readiness and response.

It is only through collaboration and communication that we can be successful in helping to protect and secure the critical infrastructure that supports all of our citizens and businesses.

National

They certainly do!



ShmooCon 2009

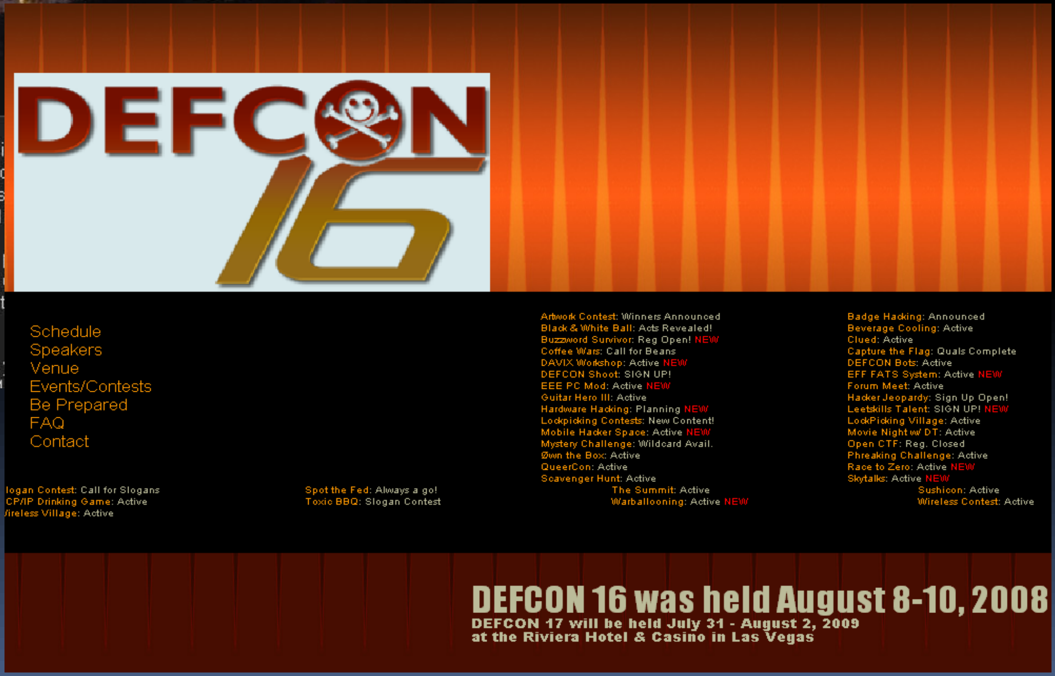
Feb 6 - 8, Wardman Park Marriott, Washington DC, USA

Welcome

Different • ShmooCon is an annual East coast hacker conventi
interesting atmosphere for demonstrating technology exploitatio
and open discussions of critical infosec issues. The first day is
Mind. The next two days, there are three tracks: Break It!, Buil

Affordable • ShmooCon is about high-quality without the high
registration discounts, and ShmooCon can be dirt cheap. Spac
last two years, so unless taking a chance on an eBay auction t
early!

Accessible • Well, except for our West coast friends, sorry gu
Marriott Wardman Park Hotel, just a few steps from the D.C. M



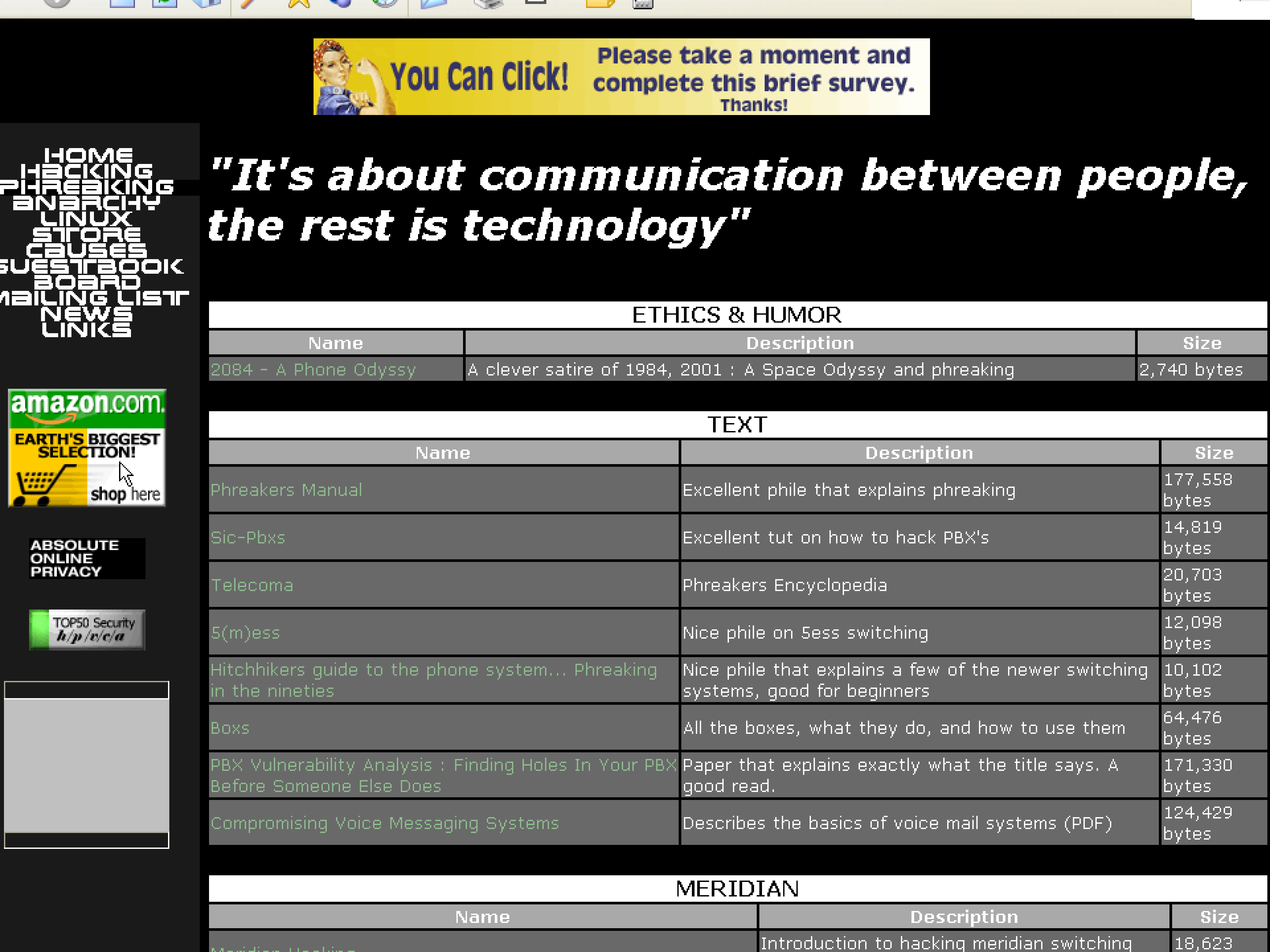
Artwork Contest: Winners Announced
Black & White Ball: Acts Revealed!
Buzzword Survivor: Reg Open! NEW
Coffee Wars: Call for Beans
DAVIX Workshop: Active NEW
DEFCON Shoot: SIGN UP!
EEE PC Mod: Active NEW
Guitar Hero III: Active
Hardware Hacking: Planning NEW
Lockpicking Contests: New Content!
Mobile Hacker Space: Active NEW
Mystery Challenge: Wildcard Avail.
Øwn the Box: Active
QueerCon: Active
Scavenger Hunt: Active
The Summit: Active
Warballooning: Active NEW

Badge Hacking: Announced
Beverage Cooling: Active
Clued: Active
Capture the Flag: Quals Complete
DEFCON Bots: Active
EFF FATS System: Active NEW
Forum Meet: Active
Hacker Jeopardy: Sign Up Open!
Leetskills Talent: SIGN UP! NEW
LockPicking Village: Active
Movie Night w/ DT: Active
Open CTF: Reg. Closed
Phreaking Challenge: Active
Race to Zero: Active NEW
Skytalks: Active NEW
Sushicon: Active
Wireless Contest: Active

logan Contest: Call for Slogans
CP/IP Drinking Game: Active
/ireless Village: Active

Spot the Fed: Always a go!
Toxic BBQ: Slogan Contest

DEFCON 16 was held August 8-10, 2008
DEFCON 17 will be held July 31 - August 2, 2009
at the Riviera Hotel & Casino in Las Vegas



"It's about communication between people, the rest is technology"

ETHICS & HUMOR

Name	Description	Size
2084 - A Phone Odyssy	A clever satire of 1984, 2001 : A Space Odyssy and phreaking	2,740 bytes

TEXT

Name	Description	Size
Phreakers Manual	Excellent phile that explains phreaking	177,558 bytes
Sic-Pbxs	Excellent tut on how to hack PBX's	14,819 bytes
Telecoma	Phreakers Encyclopedia	20,703 bytes
5(m)ess	Nice phile on 5ess switching	12,098 bytes
Hitchhikers guide to the phone system... Phreaking in the nineties	Nice phile that explains a few of the newer switching systems, good for beginners	10,102 bytes
Boxs	All the boxes, what they do, and how to use them	64,476 bytes
PBX Vulnerability Analysis : Finding Holes In Your PBX Before Someone Else Does	Paper that explains exactly what the title says. A good read.	171,330 bytes
Compromising Voice Messaging Systems	Describes the basics of voice mail systems (PDF)	124,429 bytes

MERIDIAN

Name	Description	Size
Meridian Hacking	Introduction to hacking meridian switching	18,623

"No matter what kind of shop you run, Linux, Mac or Windows, you are exposed to a variety of security threats on a daily basis. You have to deal with potential information spills, security breaches and system compromises, as well as fighting the propensity of humans to do incredibly foolish things."

Linda LeBlanc
Former Gunnery Sergeant, U.S. Marine Corps

The opposing team?

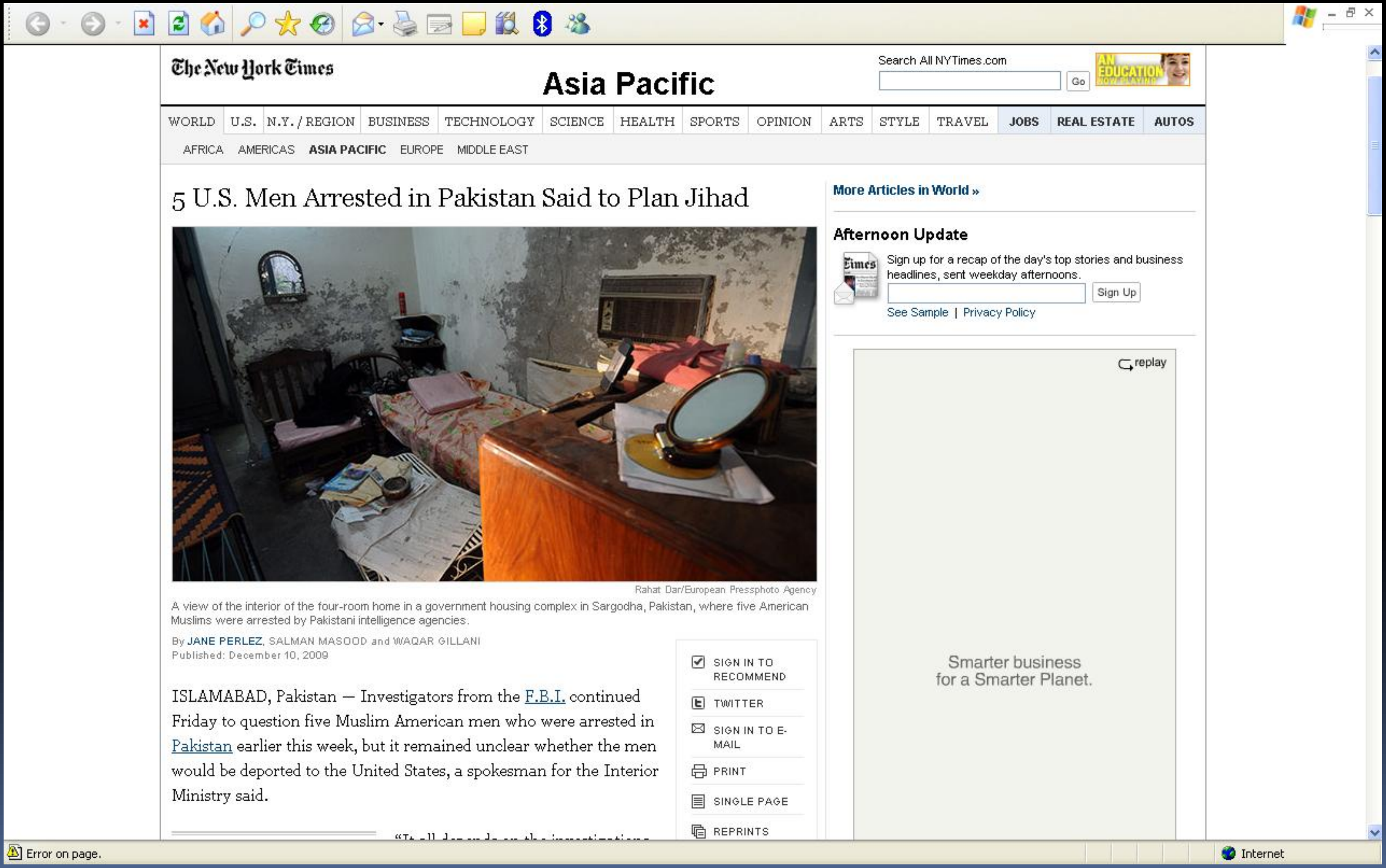
- The Hackers
- Disgruntled Insiders
- Clueless employees
- Competitors
- Foreign Governments
- Terror organizations

Terrorists

- There are 154 known Terror Organizations
- They have two things in common:

1. A visceral hatred of the United States and our freedoms
2. They are using the Internet for command, control, communications and recruitment

Did I mention recruitment



5 U.S. Men Arrested in Pakistan Said to Plan Jihad

Rahat Dar/European Pressphoto Agency

A view of the interior of the four-room home in a government housing complex in Sargodha, Pakistan, where five American Muslims were arrested by Pakistani intelligence agencies.

By JANE PERLEZ, SALMAN MASOOD and WAQAR GILLANI
Published: December 10, 2009

ISLAMABAD, Pakistan — Investigators from the F.B.I. continued Friday to question five Muslim American men who were arrested in Pakistan earlier this week, but it remained unclear whether the men would be deported to the United States, a spokesman for the Interior Ministry said.

“It all depends on the investigations

Afternoon Update

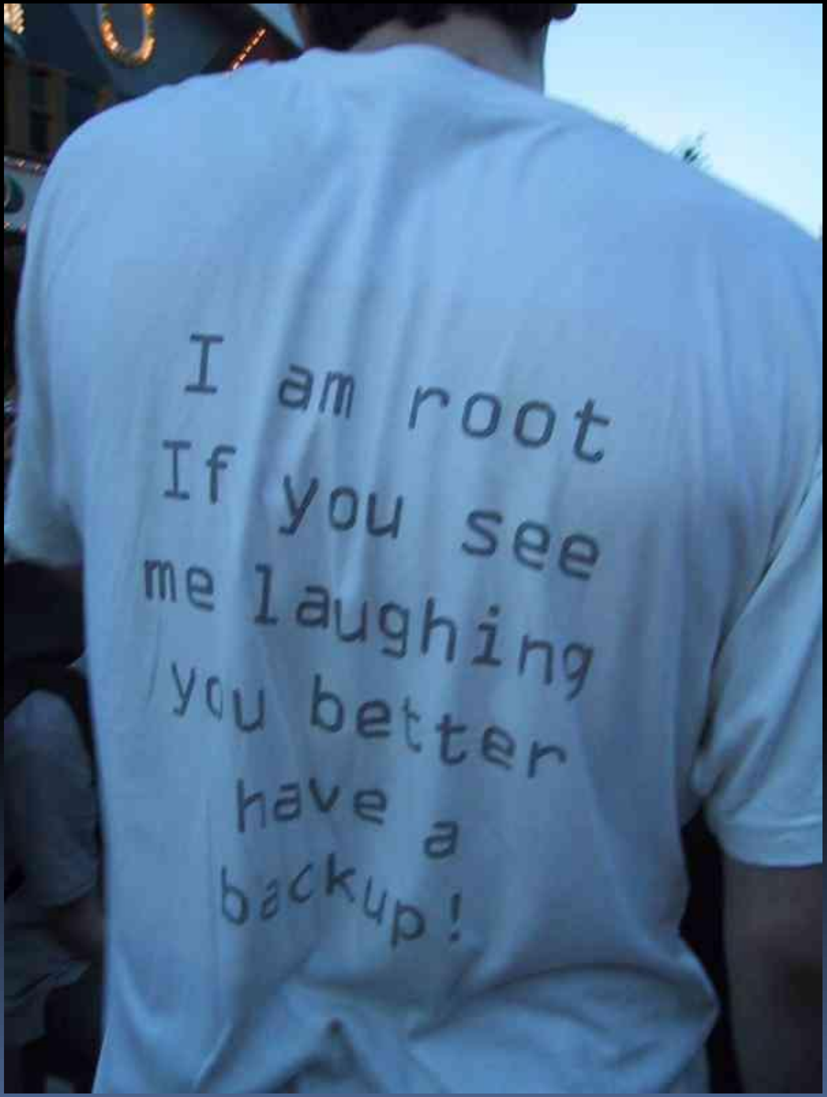
Sign up for a recap of the day's top stories and business headlines, sent weekday afternoons.

Sign Up

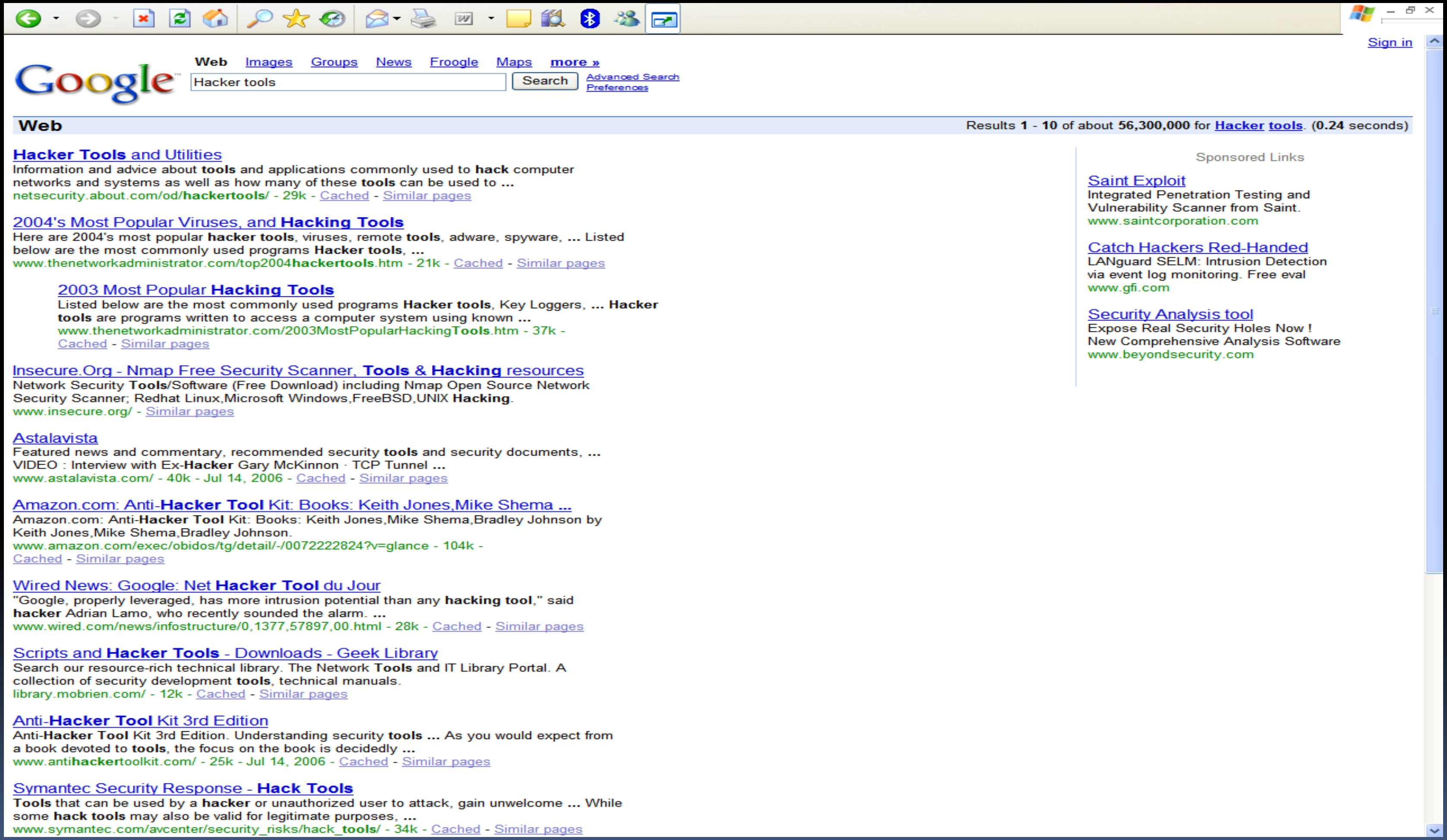
See Sample | Privacy Policy

The Hackers

The Hacker Threat



The Tools



Hacker tools

Web Results **1** - **10** of about **56,300,000** for **Hacker tools**. (**0.24** seconds)

Hacker Tools and Utilities
Information and advice about **tools** and applications commonly used to **hack** computer networks and systems as well as how many of these **tools** can be used to **...**
netsecurity.about.com/od/**hackertools**/ - 29k - Cached - Similar pages

2004's Most Popular Viruses, and **Hacking Tools**
Here are 2004's most popular **hacker tools**, viruses, remote **tools**, adware, spyware, **...** Listed below are the most commonly used programs **Hacker tools**, **...**
www.thenetworkadministrator.com/top2004**hackertools**.htm - 21k - Cached - Similar pages

2003 Most Popular **Hacking Tools**
Listed below are the most commonly used programs **Hacker tools**, Key Loggers, **... Hacker tools** are programs written to access a computer system using known **...**
www.thenetworkadministrator.com/2003MostPopularHacking**Tools**.htm - 37k - Cached - Similar pages

Insecure.Org - Nmap Free Security Scanner, **Tools** & **Hacking** resources
Network Security **Tools**/Software (Free Download) including Nmap Open Source Network Security Scanner; Redhat Linux,Microsoft Windows,FreeBSD,UNIX **Hacking**.
www.insecure.org/ - Similar pages

Astalavista
Featured news and commentary, recommended security **tools** and security documents, **...** VIDEO : Interview with Ex-**Hacker** Gary McKinnon · TCP Tunnel **...**
www.astalavista.com/ - 40k - Jul 14, 2006 - Cached - Similar pages

Amazon.com: Anti-**Hacker Tool** Kit: Books: Keith Jones,Mike Shema **...**
Amazon.com: Anti-**Hacker Tool** Kit: Books: Keith Jones,Mike Shema,Bradley Johnson by Keith Jones,Mike Shema,Bradley Johnson.
www.amazon.com/exec/obidos/tg/detail/-/0072222824?v=glance - 104k - Cached - Similar pages

Wired News: Google: Net **Hacker Tool** du Jour
"Google, properly leveraged, has more intrusion potential than any **hacking tool**," said **hacker** Adrian Lamo, who recently sounded the alarm. **...**
www.wired.com/news/infostructure/0,1377,57897,00.html - 28k - Cached - Similar pages

Scripts and **Hacker Tools** - Downloads - Geek Library
Search our resource-rich technical library. The Network **Tools** and IT Library Portal. A collection of security development **tools**, technical manuals.
library.mobrien.com/ - 12k - Cached - Similar pages

Anti-**Hacker Tool** Kit 3rd Edition
Anti-**Hacker Tool** Kit 3rd Edition. Understanding security **tools ...** As you would expect from a book devoted to **tools**, the focus on the book is decidedly **...**
www.anti**hacker**toolkit.com/ - 25k - Jul 14, 2006 - Cached - Similar pages

Symantec Security Response - **Hack Tools**
Tools that can be used by a **hacker** or unauthorized user to attack, gain unwelcome **...** While some **hack tools** may also be valid for legitimate purposes, **...**
www.symantec.com/avcenter/security_risks/hack_tools/ - 34k - Cached - Similar pages

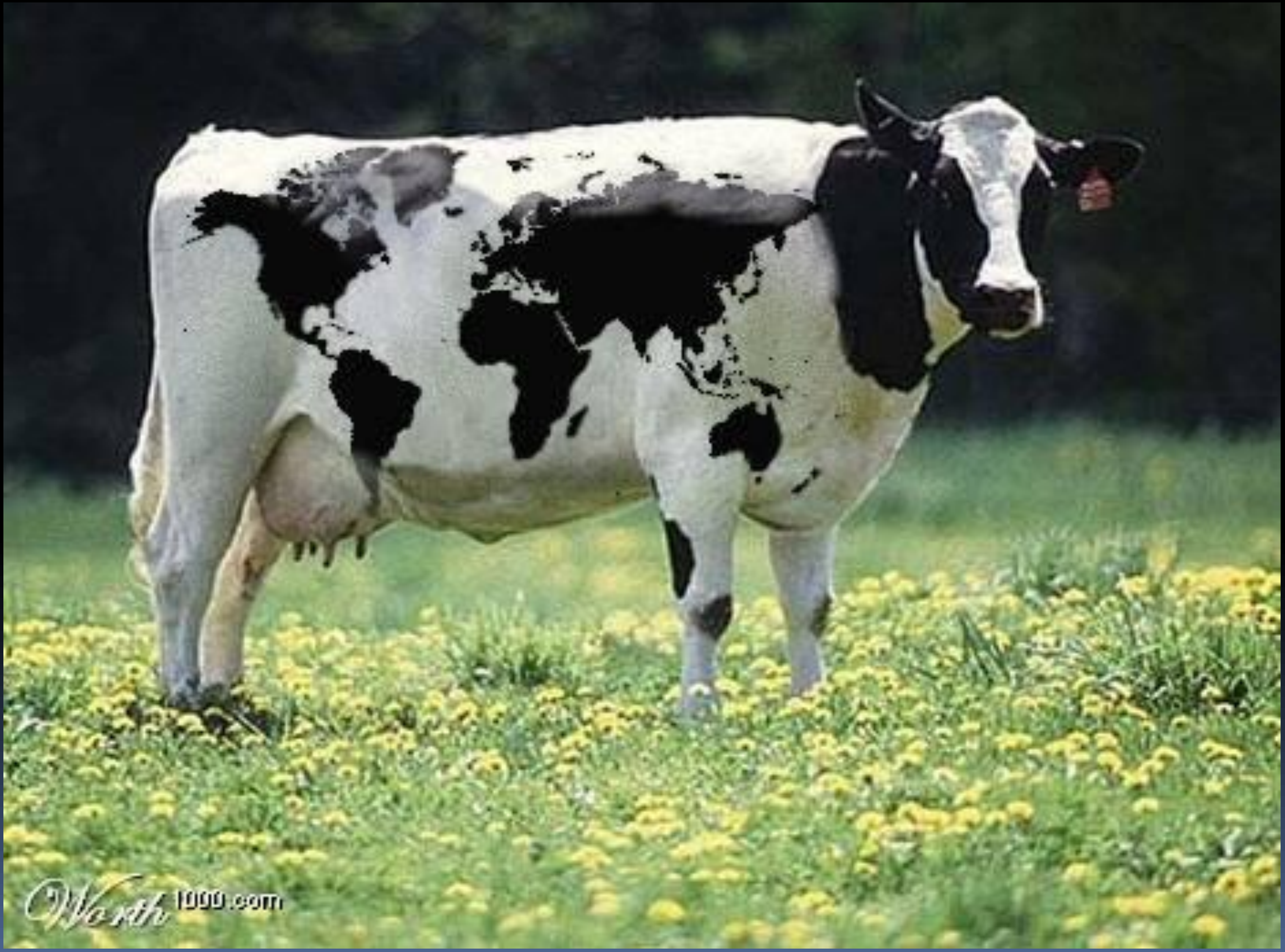
Sponsored Links

Saint Exploit
Integrated Penetration Testing and Vulnerability Scanner from Saint.
www.saintcorporation.com

Catch Hackers Red-Handed
LANguard SELM: Intrusion Detection via event log monitoring. Free eval
www.gfi.com

Security Analysis tool
Expose Real Security Holes Now ! New Comprehensive Analysis Software
www.beyondsecurity.com

Remember, this is a global phenomenon, it’s not just about Sacramento



Biggest Players in the Global Black Market

- Russia
- China
- France
- Israel
- U.S.

Krews

- HangUp Team
- CNHonker
- Russian Business Network
- Rock Phish
- 76Service
- MAAS
- Hoff is Thirsty

Their Motivation?

Top 8 Perceived Threats

- System penetration
- Sabotage of data
- Theft of proprietary information
- Denial of service
- Viruses and Worms
- Unauthorized insider access
- Laptop theft
- Insider abuse of the Internet

System Penetration

- It is an unfortunate reality that you will suffer a breach of security at some point
- To bypass security, an attacker only has to find one vulnerable system within the entire network
- But to guarantee security, you have to make sure that 100 percent of your systems are invulnerable -- 100 percent of the time

Data Leakage:
How many instances in 2009?

- 526 instances of Data Leakage
- 39,664,641 individuals affected and counting
- Lots of unhappy people
- How will you be impacted?

Public Sector

- Bluegrass Community and Technical College (Danville, KY)
- Naval Hospital Pensacola, FL
- School for the Physical City (New York, NY)
- University Florida
- Akron Children's Hospital (Akron, OH)
- Eastern Kentucky University (Richmond, KY)

Public Sector

- UNC Chapel Hill (Chapel Hill, NC)
- Suffolk Community College (Selden, NY)
- U.S. Army Special Forces (Fort Bragg, NC)
- Pitt County Memorial Hospital (Greenville, NC)
- Virginia Department of Education
- Bullitt County Public Schools (Shepherdsville, KY)
- Roane State Community College (Harriman, TN)

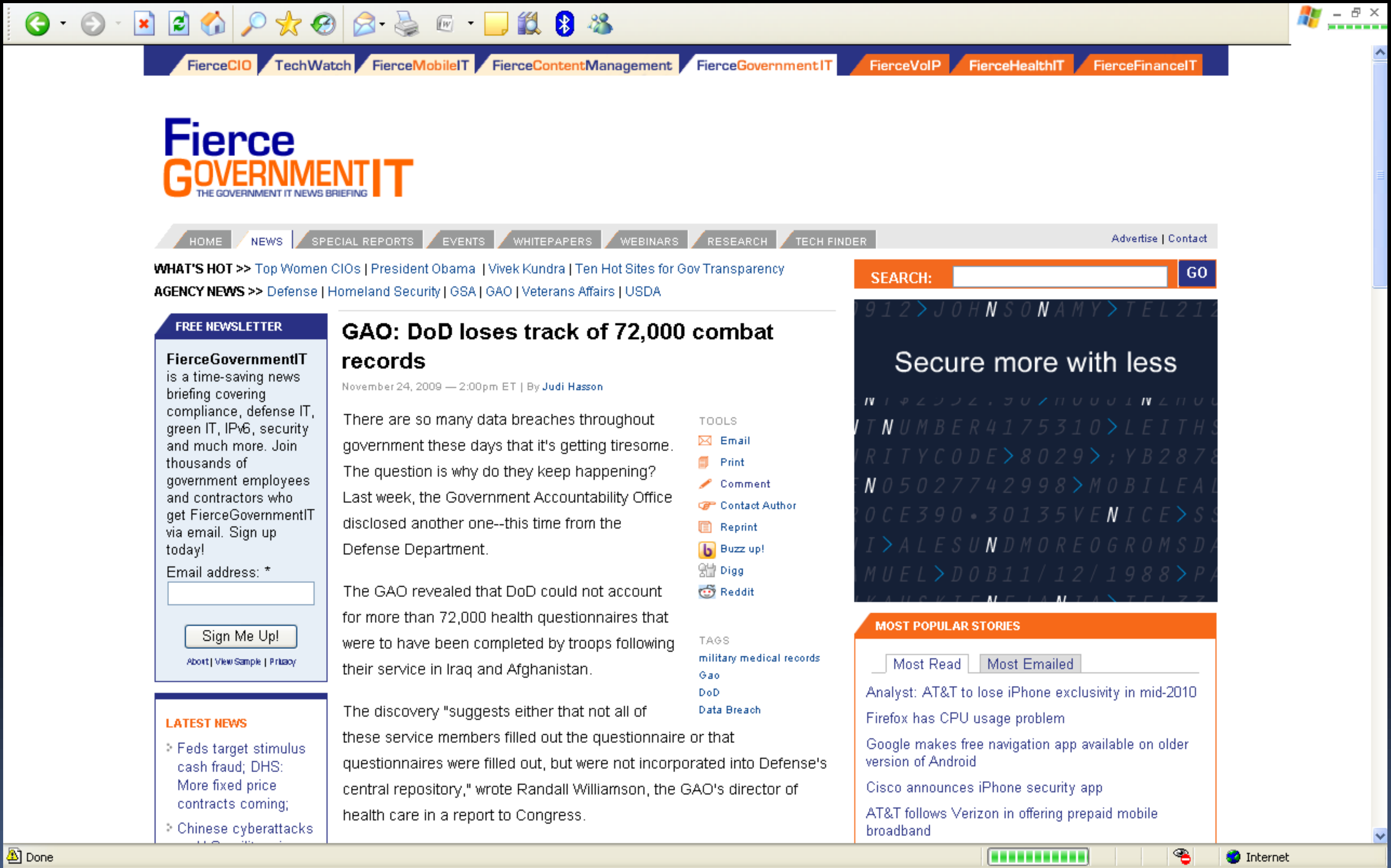
Public Sector

- Chaminade University (Honolulu, HI)
- National Archives and Records Administration (College Park, MD)
- Nebraska Workers' Compensation Court (Omaha, NE)
- University Medical Center (Las Vegas, NV)
- Penn State (University Park, PA)

Public Sector

- Salem Housing and Community Services (Salem, OR)
- Eastern Illinois University (Charleston, IL)
- University of Nebraska (Omaha, NE)
- Wake County Schools (Raleigh, NC)
- Bushland Elementary School (Bushland, TX)
- University Medical Center (Las Vegas, NV)

Public Sector Last 90 Days



WHAT'S HOT >> Top Women CIOs | President Obama | Vivek Kundra | Ten Hot Sites for Gov Transparency

AGENCY NEWS >> Defense | Homeland Security | GSA | GAO | Veterans Affairs | USDA

FREE NEWSLETTER

FierceGovernmentIT is a time-saving news briefing covering compliance, defense IT, green IT, IPv6, security and much more. Join thousands of government employees and contractors who get FierceGovernmentIT via email. Sign up today!

Email address: *

About | View Sample | Privacy

LATEST NEWS

- Feds target stimulus cash fraud; DHS: More fixed price contracts coming;
- Chinese cyberattacks

GAO: DoD loses track of 72,000 combat records

November 24, 2009 — 2:00pm ET | By Judi Hasson

There are so many data breaches throughout government these days that it's getting tiresome. The question is why do they keep happening? Last week, the Government Accountability Office disclosed another one--this time from the Defense Department.

The GAO revealed that DoD could not account for more than 72,000 health questionnaires that were to have been completed by troops following their service in Iraq and Afghanistan.

The discovery "suggests either that not all of these service members filled out the questionnaire or that questionnaires were filled out, but were not incorporated into Defense's central repository," wrote Randall Williamson, the GAO's director of health care in a report to Congress.

TOOLS

- Email
- Print
- Comment
- Contact Author
- Reprint
- Buzz up!
- Digg
- Reddit

TAGS

military medical records
Gao
DoD
Data Breach

MOST POPULAR STORIES

Analyst: AT&T to lose iPhone exclusivity in mid-2010

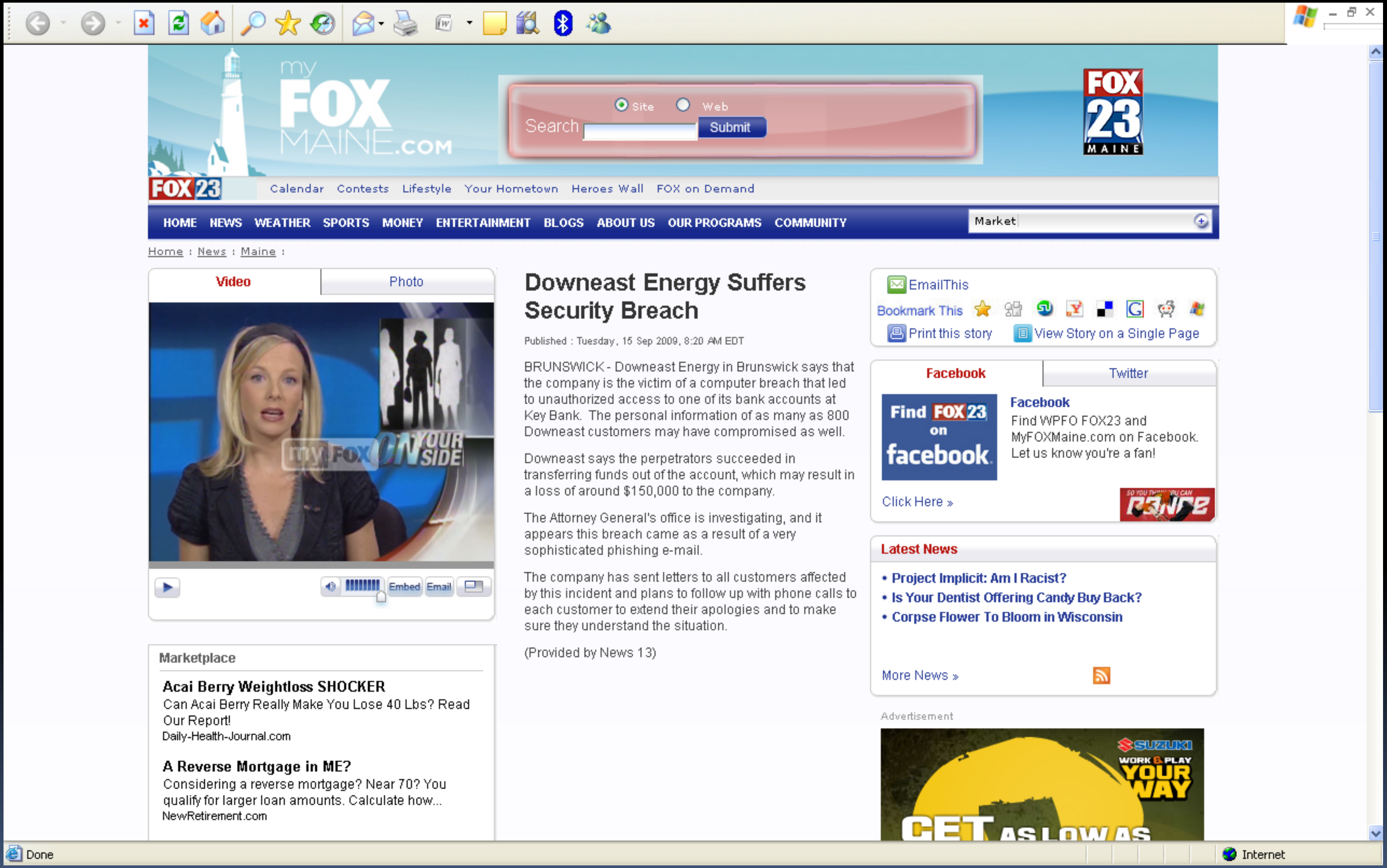
Firefox has CPU usage problem

Google makes free navigation app available on older version of Android

Cisco announces iPhone security app

AT&T follows Verizon in offering prepaid mobile broadband

Ouch!



myFOX MAINE.COM
Search ● Site ○ Web Submit
FOX 23 MAINE
Calendar Contests Lifestyle Your Hometown Heroes Wall FOX on Demand
HOME NEWS WEATHER SPORTS MONEY ENTERTAINMENT BLOGS ABOUT US OUR PROGRAMS COMMUNITY
Market
Home : News : Maine :
Video Photo
myFOX ON YOUR SIDE
Embed Email
EmailThis
Bookmark This
Print this story
View Story on a Single Page
Facebook Twitter
Find FOX23 on facebook
Click Here »
Done
Internet

Downeast Energy Suffers Security Breach

Published : Tuesday, 15 Sep 2009, 8:20 AM EDT

BRUNSWICK - Downeast Energy in Brunswick says that the company is the victim of a computer breach that led to unauthorized access to one of its bank accounts at Key Bank. The personal information of as many as 800 Downeast customers may have compromised as well.

Downeast says the perpetrators succeeded in transferring funds out of the account, which may result in a loss of around $150,000 to the company.

The Attorney General's office is investigating, and it appears this breach came as a result of a very sophisticated phishing e-mail.

The company has sent letters to all customers affected by this incident and plans to follow up with phone calls to each customer to extend their apologies and to make sure they understand the situation.

(Provided by News 13)

Facebook

Find WPFO FOX23 and MyFOXMaine.com on Facebook. Let us know you're a fan!

Latest News

- Project Implicit: Am I Racist?
- Is Your Dentist Offering Candy Buy Back?
- Corpse Flower To Bloom in Wisconsin

More News »

Anatomy of an attack

- Last month, Brunswick, Maine-based heating and hardware firm **Downeast Energy & Building Supply** sent a letter notifying at least 850 customers that the company had suffered a data breach
- Downeast sent the notice after discovering that hackers had broken in and stolen more than $200,000 from the company's online bank account
- The hackers gained entrance when a Downeast employee clicked on a hyperlink in a fraudulent email

First inkling to Downeast

- The first indications of fraud came when Downeast's chief financial officer received a phone call from a bank in Texas, asking whether the company had approved a suspicious transfer to a local resident in the amount of $9,800

Utilizing “Money Mules”

- Utilizing a keylogger the hackers used that access to initiate a series of sub-$10,000 money transfers out of the company's account to at least 20 individuals around the United States

Western Union

- The mules are then instructed to withdraw the cash and wire it via Western Union or Moneygram to fraud gangs overseas, typically in Eastern Europe
- It is not uncommon for a single cyber robbery to depend on the help of dozens of money mules

The Duped

- One individual who received the funds from Downeast's account was Kenneth Durastanti, a 24-year-old Ball, LA resident who was recently recruited by a company called Entrust Group Inc

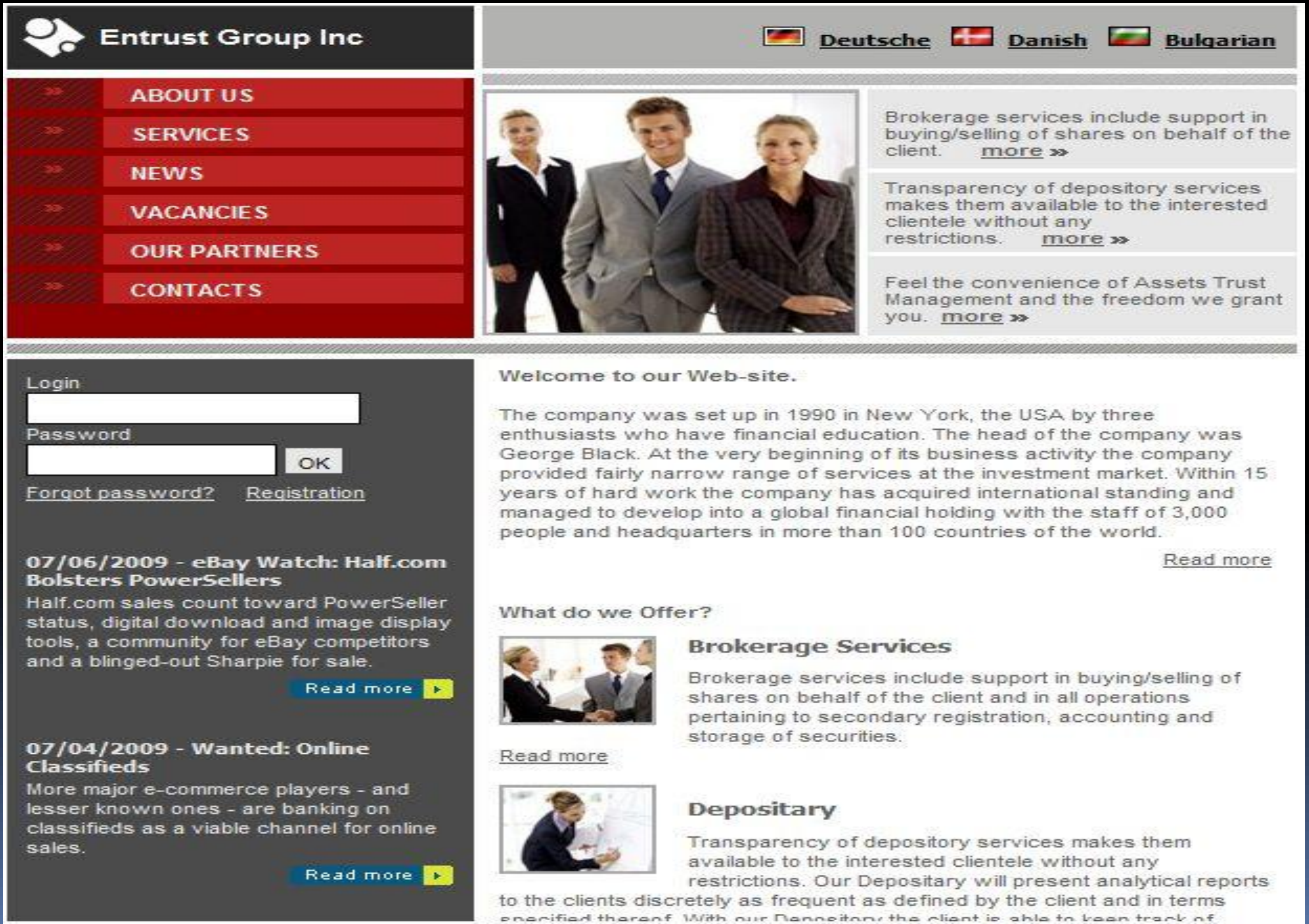
$$$$$$

- Entrust Group told him they had found his resume on Careerbuilder.com, and that Kenneth could make thousands of dollars a month working from home

Bogus or what?

- The company claims to be a 19-year-old brokerage firm located in Rochester, N.Y., but there is no listing for a company by that name in the New York State business register
- Also, the company's Web site is hosted in China, and its domain name -- www.entrust-groupsvc.cn
- We call that a clue

The Internet Advertisement



Brokerage services include support in buying/selling of shares on behalf of the client. more »

Transparency of depository services makes them available to the interested clientele without any restrictions. more »

Feel the convenience of Assets Trust Management and the freedom we grant you. more »

07/06/2009 - eBay Watch: Half.com Bolsters PowerSellers

Half.com sales count toward PowerSeller status, digital download and image display tools, a community for eBay competitors and a blinged-out Sharpie for sale.

Read more

07/04/2009 - Wanted: Online Classifieds

More major e-commerce players - and lesser known ones - are banking on classifieds as a viable channel for online sales.

Read more

Welcome to our Web-site.

The company was set up in 1990 in New York, the USA by three enthusiasts who have financial education. The head of the company was George Black. At the very beginning of its business activity the company provided fairly narrow range of services at the investment market. Within 15 years of hard work the company has acquired international standing and managed to develop into a global financial holding with the staff of 3,000 people and headquarters in more than 100 countries of the world.

Read more

What do we Offer?

Brokerage Services

Brokerage services include support in buying/selling of shares on behalf of the client and in all operations pertaining to secondary registration, accounting and storage of securities.

Read more

Depositary

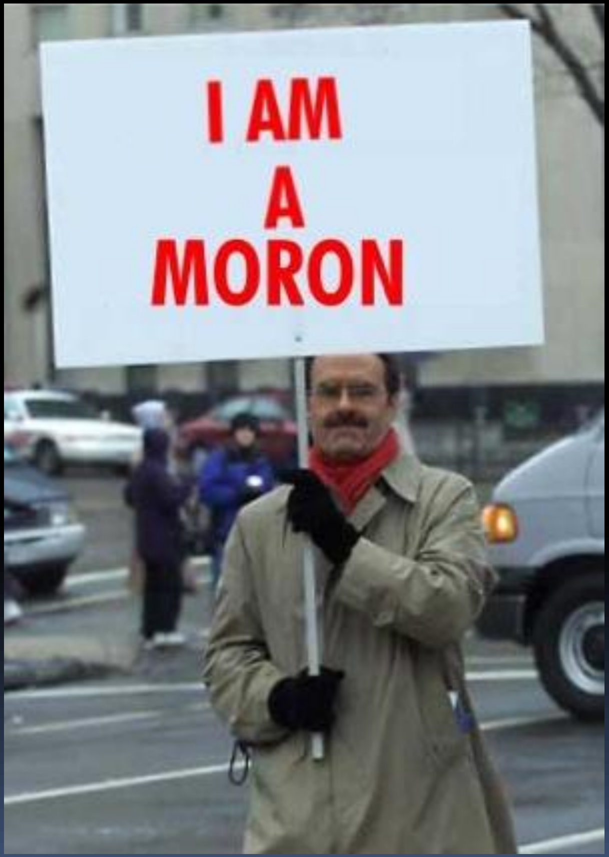
Transparency of depository services makes them available to the interested clientele without any restrictions. Our Depositary will present analytical reports to the clients discretely as frequent as defined by the client and in terms specified thereof. With our Depository the client is able to keep track of

Too good too be true

- Kenneth's mother warned him it was too good to be true
- Entrust told Kenneth that they wanted his bank account number and ID so they could put a large sum of money in his account
- They wired a $9,589 transfer to his account and he was directed to send a Western Union Moneygram to individuals in the Ukraine

A moron gets lucky

- Instead of sending the money to the Ukraine, he accidently sent it to himself
- His stupidity saved him from prosecution



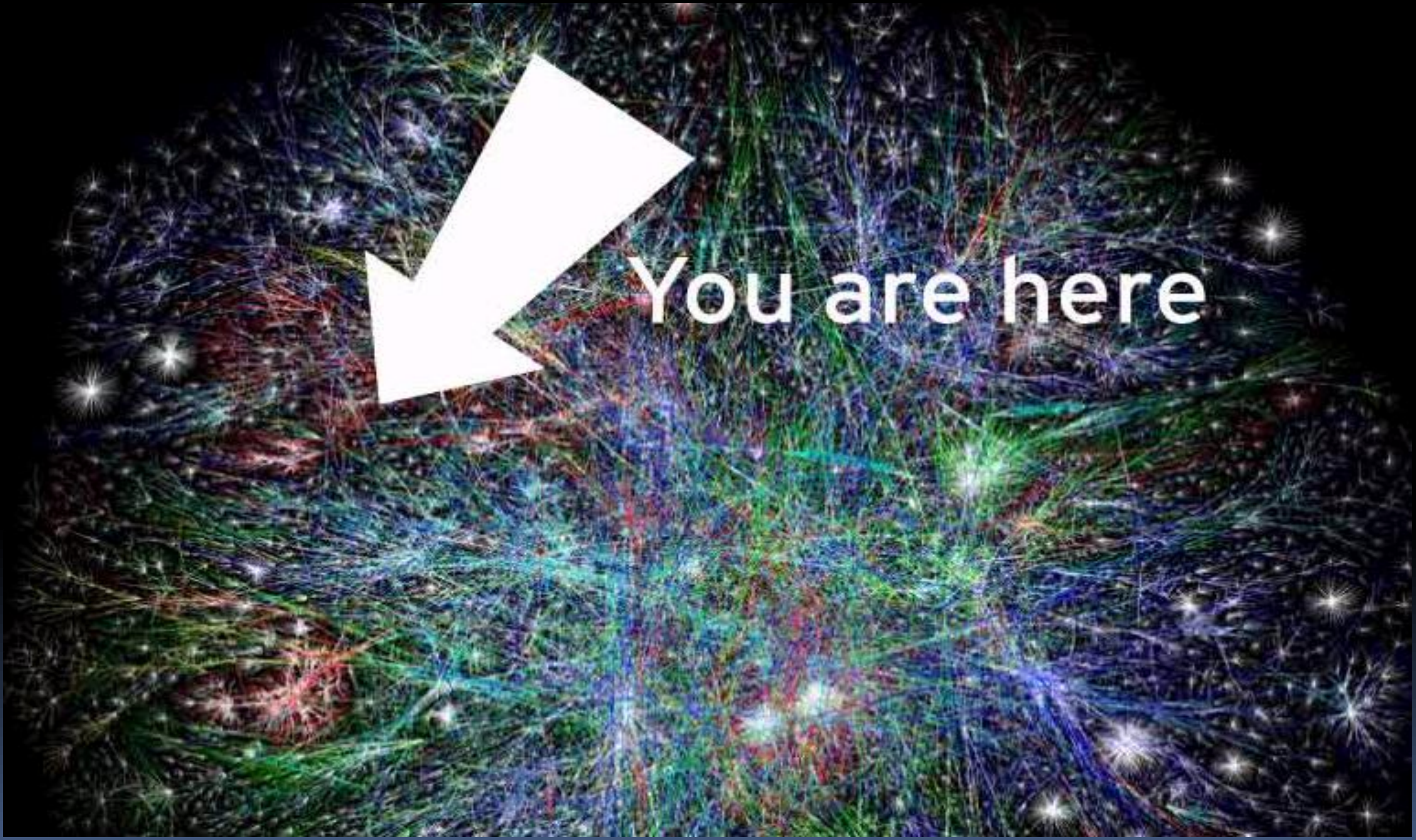
Not good…

- But Patrick! It won’t happen to us!

Whether you get hacked depends…

- Do you assume the posture of, “It can’t happen here.”
- Do you hear, “We haven’t heard of any worm outbreaks and all seems quiet. Why upgrade those devices?”
- “We have no budget.”
- “We’re just hanging out in Sacramento!”
- “They’re only going after the U.S. Government and those really big banks.”
- Then my question is, “Can you really afford to give up data today?

Welcome to the Borderless Network

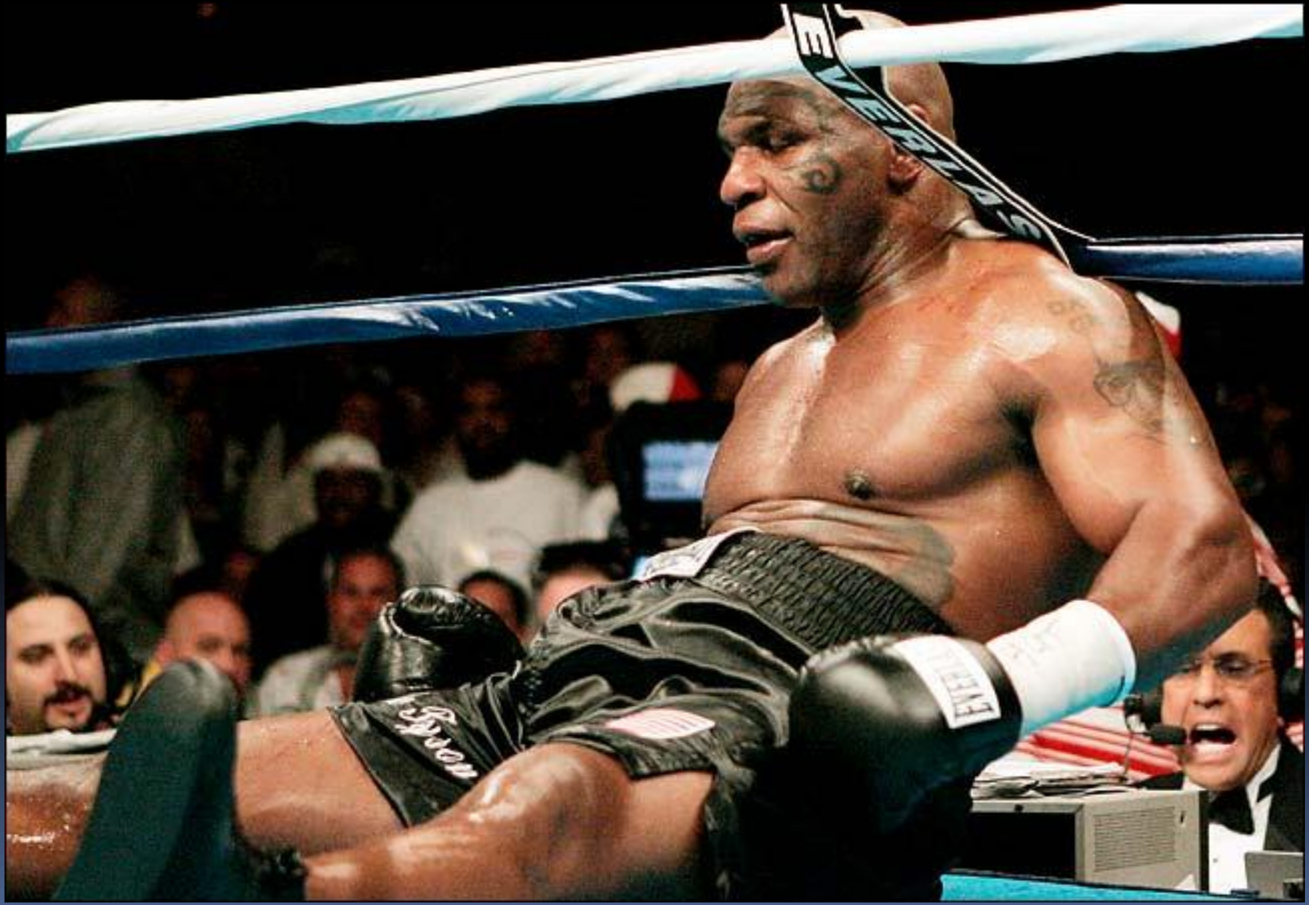


So,

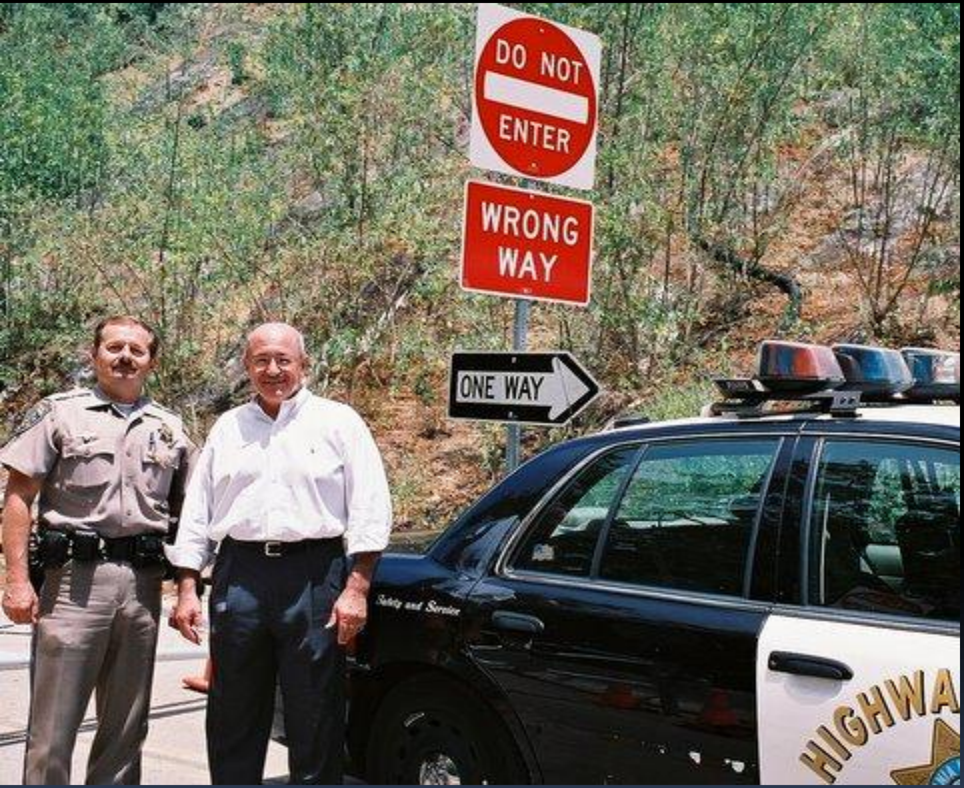
- Be compliant but don’t rest on your laurels
- Be vigilant
- Educate
- Know that you are a target
- Be ready to respond

How true!

- “Every man has a plan, until he gets hit!”



Know who to call…

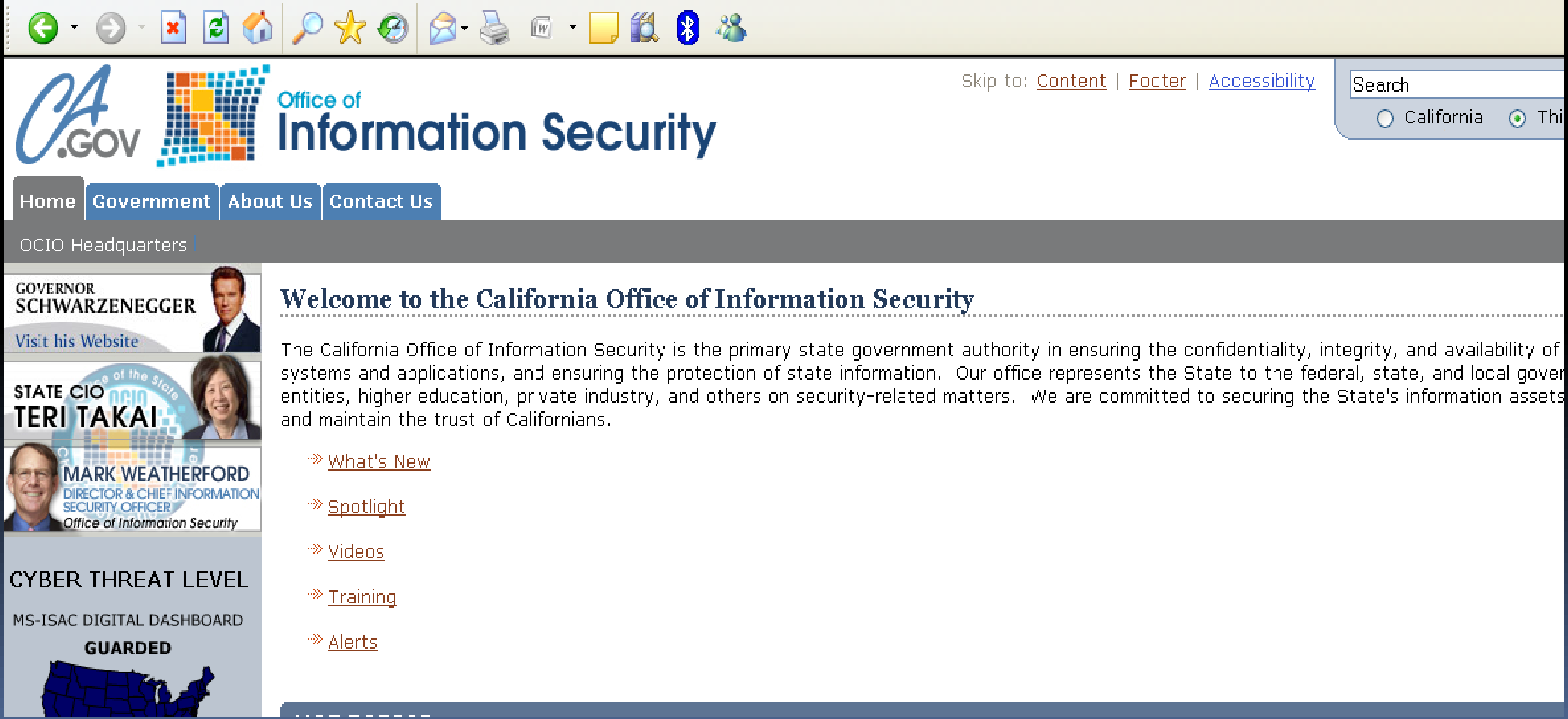


And in closing…

Let’s not monkey around, protect California’s data now!

It’s up to you…

- Your policy – let’s make sure we honor our pledge to the residents of California



Welcome to the California Office of Information Security

The California Office of Information Security is the primary state government authority in ensuring the confidentiality, integrity, and availability of systems and applications, and ensuring the protection of state information. Our office represents the State to the federal, state, and local gover entities, higher education, private industry, and others on security-related matters. We are committed to securing the State's information assets and maintain the trust of Californians.

- What's New
- Spotlight
- Videos
- Training
- Alerts

A great plan!

California Information Security Strategic Plan

October

2009

Thanks very much and please, no risky behavior on State PCs!

Public Service Announcement – If you see this man, dial 911 – do not approach alone

From an old U.S. Marine…

For those who have served, thanks!

Graphic by
WTC Stephen Harris, USN Ret.